

Australian Standard<sup>®</sup>

**Application of Markov techniques**



This Australian Standard® was prepared by Committee QR-005, Dependability. It was approved on behalf of the Council of Standards Australia on 16 June 2008. This Standard was published on 28 July 2008.

---

The following are represented on Committee QR-005:

- AirServices Australia
  - Australian Chamber of Commerce and Industry
  - Australian Electrical and Electronic Manufacturers Association
  - Australian Industry Group
  - Australian Nuclear Science & Technology Organisation
  - Australian Organisation for Quality
  - Certification Interests (Australia)
  - Department of Defence (Australia)
  - Energy Networks Association
  - Engineers Australia
  - The University of New South Wales
- 

This Standard was issued in draft form for comment as DR 08031.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

---

#### Keeping Standards up-to-date

Australian Standards® are living documents that reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued.

Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting [www.standards.org.au](http://www.standards.org.au)

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at [mail@standards.org.au](mailto:mail@standards.org.au), or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

---

Australian Standard<sup>®</sup>

## **Application of Markov techniques**

First published as AS IEC 61165—2008.

### **COPYRIGHT**

© Standards Australia

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Published by Standards Australia GPO Box 476, Sydney, NSW 2001, Australia

ISBN 0 7337 8838 6

## PREFACE

This Standard was prepared by the Standards Australia Committee QR-005, Dependability.

The objective of this Standard is to provide guidance on the application of Markov techniques to modelling and analysing a system which exhibits state-dependent behaviour and to estimating reliability, availability, maintainability and safety measures. It is suitable for use in conjunction with the AS IEC 60300 series of dependability management Standards.

This Standard is identical with, and has been reproduced from IEC 61165 Ed.2.0 (2006), *Application of Markov techniques*.

As this Standard is reproduced from an International Standard, the following applies:

- (a) Its number does not appear on each page of text and its identity is shown only on the cover and title page.
- (b) In the source text 'this International Standard' should read 'this Australia Standard.'
- (c) A full point should be substituted for a comma when referring to a decimal marker.

The terms 'normative' and 'informative' are used to define the application of the annex to which they apply. A normative annex is an integral part of a standard, whereas an informative annex is only for information and guidance.

## CONTENTS

	<i>Page</i>
INTRODUCTION .....	iv
1 Scope .....	1
2 Normative references .....	1
3 Terms and definitions .....	1
4 Symbols and abbreviations .....	3
4.1 Symbols for state transition diagrams .....	3
4.2 Other symbols and abbreviations .....	4
4.3 Example .....	5
5 General description .....	5
6 Assumptions and limitations .....	6
7 Relationship with other analysis techniques .....	7
7.1 General .....	7
7.2 Fault Tree Analysis (FTA) .....	7
7.3 Reliability Block Diagram (RBD) .....	7
7.4 Petri nets .....	8
8 Development of state transition diagrams .....	8
8.1 Prerequisites .....	8
8.2 Rules for development and representation .....	9
9 Evaluation .....	9
9.1 General .....	9
9.2 Evaluation of reliability measures .....	10
9.3 Evaluation of availability and maintainability measures .....	11
9.4 Evaluation of safety measures .....	11
10 Documentation of results .....	11
Annex A (informative) Basic mathematical relationships for Markov techniques .....	13
Annex B (informative) Example: Development of state transition diagrams .....	16
Annex C (informative) Example: Numerical evaluation of some reliability, availability, maintainability and safety measures for a 1-out-of-2 active redundant system .....	22
Bibliography .....	27

## 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.

## STANDARDS AUSTRALIA

## Australian Standard

## 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.

References to international standards that are struck through in this clause are replaced by references to Australian or Australian/New Zealand Standards that are listed immediately thereafter and identified by shading. Any Australian or Australian/New Zealand Standard that is identical to the International Standard it replaces is identified as such.

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~~

AS IEC 60300.3.1, *Dependability management—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  $P_{ij}(s, s+t) = P(X(s+t) = j | X(s) = i)$ . 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  $\Delta t$ , when  $\Delta t$  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

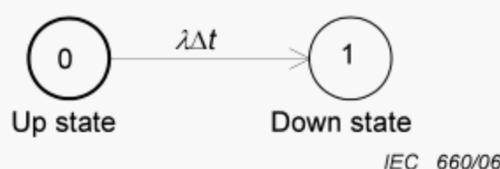
Symbols for reliability, availability, maintainability and safety measures follow those of IEC 60050(191), where available. The references below with a prefix 191 are from IEC 60050(191). In this standard the following symbols are used:

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 $t$	

Symbol/ Abbreviation	Term	Reference
$P_i$	asymptotic and steady-state probability of finding the system in state $i$ at time $t$	
$\Delta t$	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 $i$ .	

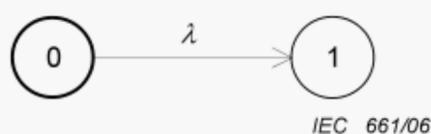
### 4.3 Example

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



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

$\lambda\Delta t$  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  $\Delta t$  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.

Provided the assumptions and limitations described in Clause 6 can be accepted, one of the major advantages of Markov techniques is that maintenance strategies, for example restoration priorities of individual elements, can be modelled. Moreover, the order in which multiple failures occur can be considered in the model. It should be noted that other analysis techniques e.g. fault tree analysis (FTA) and reliability block diagram (RBD) methods (as described in IEC 61025 and IEC 61078 respectively) do not allow complex maintenance strategies to be taken into account, though they may have special gates represented by special symbols (dynamic gates) to indicate the presence of those cases. However, the effect of those gates has to be evaluated separately by Markov techniques or other techniques, and the results included in the analysis of the Fault Tree or RBD, whilst observing the possible limitations.

Although Markov techniques, from a theoretical viewpoint, are 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 elements 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 state transition diagram (see clause 8). Also the numerical techniques used for the evaluation of the diagram can be time consuming and may require special computer programs.

Not only are Markov techniques suited to the modelling of maintenance strategies, but such methods 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.

As the number of possible states is finite, the sum of all the state probabilities is unity, i.e. at any instant in time the system can be in one – and only one – of the states in the state transition diagram. If, for practical reasons, states with very low probability are omitted, then the sum of all state probabilities is only approximately one.

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

## **6 Assumptions and limitations**

The rules given in 8.2 of this standard, for generating the state transition diagram, apply generally (apart from rule h). However, the description of numerical techniques applies only when all transition rates are constant, which implies that failure and restoration rates of all elements in the analyzed system are constant with respect to time. The assumption of constant failure rate is reasonably acceptable for components in many systems before the wear-out period (however should also be justified) but the assumption of constant restoration rate should be justified unless the mean time to restoration of elements is very small by comparison with the corresponding mean times to failure. 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 limitation arises because of the assumption used for mathematical solutions, namely, the future behaviour of the system depends only on the present state of the system, and not on the way the system arrived at this state. The analyst should ensure that this memory-less property of Markov models is a sufficient approximation of the real system behaviour (see 8.1). Special care is needed when modelling effects of common cause failures that may result in some potential intermediate states being by-passed (see Figure B.4).

The usual assumptions for each element in the system considered can be summarised as follows:

- the failure rate,  $\lambda$ , and the restoration rate,  $\mu$ , are constant (time-independent);
- the transition probability from a state  $i$  to a state  $j$  within the small time interval  $(t, t+\Delta t)$  given that the system is in state  $i$  at time  $t$  is  $q_{ij} \Delta t$ , where  $q_{ij}$  is a sum of failure and restoration rates of involved elements.

NOTE Theoretically the limitation with respect to the constant failure and restoration rates can often be overcome at the expense of expansion of the state space, as many non-exponential distribution of times to failure or to restore can be approximated by a sum of exponential distributions. Each of these exponential distributions has to be modelled as an additional state, which acts as a kind of memory for the elapsed time to failure or time to restore. However, this concept, usually called phase (or supplementary states) concept, has not been widely put into practice.

## 7 Relationship with other analysis techniques

### 7.1 General

Markov techniques can be used to model events or states in other modelling techniques, in particular, when these other techniques lack certain capabilities which Markov techniques have, e. g. the ability to express time or state dependent behaviour. The resulting models are often called hybrid models.

A comprehensive discussion of modelling techniques is given in IEC 60300-3-1. A full discussion on hybrid models is left to the standards which utilize Markov state transition diagrams for this purpose, e.g. IEC 61078 or IEC 61025. The purpose of this clause is to give some general considerations for hybrid models.

### 7.2 Fault Tree Analysis (FTA)

FTA can be used to evaluate the probability of a failure at a given instant  $t$  in time using Boolean logic. This logic may not express time or state dependencies properly. In these cases it is possible to extend FTA by creating new gates, which represent particular Markov models, which are separately evaluated and hide the actual Markov model from the user. Such gates bear the name of "Dynamic" gates, for example PRIORITY AND, SEQUENTIAL INHIBIT or SPARE gate. Each of such gates may be replaced by a basic event with the probability of occurrence as calculated from the Markov technique. The resulting model is often called hybrid or dynamic FTA.

Both static and dynamic gates of a fault tree can be modelled by Markov techniques. However, particular attention shall be paid to independence properties between the events in the Markov model and the events in the fault tree. In the fault tree, the parts evaluated by Markov techniques have to be assumed to be independent branches.

### 7.3 Reliability Block Diagram (RBD)

A RBD is also a technique that may use Boolean logic and therefore has similar limitations to those of FTA.

In the RBD, it is possible to delineate the portions of the RBD (by encircling the blocks), for which the Markov model is to be used. The encircled blocks have to form a network with a single input and a single output, and must not include blocks replicated elsewhere. Further guidance is given by IEC 61078.

#### 7.4 Petri nets

Petri nets are a graphical technique for the representation and analysis of complex logical interactions among elements in a system.

A particular class of Petri nets, the General Stochastic Petri Nets (GSPN) have an equivalent modelling capability to Markov techniques. Petri nets may be regarded as a natural implicit expression of its explicit Markov model representation. Petri nets can be converted to Markov models. So General Stochastic Petri Net models containing complex interactions can often be described more easily and with a smaller diagram than using Markov techniques. For evaluation purposes, the Petri net is converted to its corresponding Markov model, which is then analyzed. In practice, this is automated by software tools.

## 8 Development of state transition diagrams

### 8.1 Prerequisites

Before starting to analyze a system, the following general tasks should be performed:

- a) Set the goal of the analysis: The first crucial question which has to be answered is what should be the objective of the analysis. This could be any one or more of the following:
- the probability that the system will fail before time  $t$ ;
  - the frequency of hazardous events;
  - the mean time before the first system failure occurs;
  - the steady-state availability;
  - the probability that the system will fail when a request for its operation is issued (for systems not in continuous use);
  - other measure, to be specified.

The unit of measurement also needs to be defined.

- b) Define the characteristics of the system and the boundary conditions of the analysis. Here questions such as the following need to be answered:
- what are the important features of the system which need to be modelled?
  - how can these features be validated or at least be checked for plausibility?
  - will the system be restored (after a failure) or not?
  - is it necessary to describe time-dependent behaviour?
  - what is the actual uncertainty of the data, e.g. failure and restoration rates, or common-cause factors?
  - what is the required accuracy and/or confidence level of the results?

If some features of the real world system are not important for the model this should be justified.

- c) make sure that the Markov technique is the most appropriate analysis technique for the task. The choice of technique should be based on the objectives of the analysis and the characteristics of the system, not vice versa; otherwise certain characteristics of the system may not be modelled at all. In particular the assumptions and limitations of the model need to be carefully checked.
- d) the model and the input data should be reviewed by experts (practitioners with field experience), because errors or inaccuracies in the model or the data could have a high impact on the result of the analysis.

A critical task in Markov analysis is the proper design of the state transition diagram. Subclause 8.2 gives some recommended rules. The rules should be established before the analysis is undertaken and hence should provide for a proper identification of the individual states. This will enable construction of clear graphical models.

## 8.2 Rules for development and representation

The rules below are given as a guide for the systematic development of state transition diagrams. State transition diagrams following these rules will allow easy comprehension and comparison. Other symbols or diagram arrangements may be more suitable in some instances.

- a) the state should be depicted by a circle or rectangle with identification which allows the numerical 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 state symbol should include a clear description of the state, either directly or by reference to an explanatory list.
- c) states should be arranged so that the leftmost state is an up state and the rightmost state is a down 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 restoration.
- d) system states corresponding to the same number of down elements 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 an explanatory list.
- g) where possible, each transition should link only neighbouring state symbols. If a common cause failure disables simultaneously two or more elements, a state needs to be by-passed.
- h) to increase readability, down states at system level can be highlighted (e.g. by bold lines, colouring or hatching).

The application of these rules is illustrated in Annex B.

## 9 Evaluation

### 9.1 General

The purpose in evaluating the state transition diagram is to determine the reliability, availability, maintainability or safety measures of the system. The evaluation uses well-known mathematical techniques (see annexes A to C). Note that the task of obtaining transient (time dependent) measures, e.g.  $R(t)$  and  $A(t)$ , requires considerably more computational effort than that of obtaining a steady-state measure  $A$  or mean values, e.g. MTTF, MDT, MUT. An example for the calculation of transient measures is given in Annex C.

At the start of the analysis, one should decide whether the main objective in the state transition diagram evaluation is to obtain transient or steady state values of the state probabilities. Although for availability investigations the latter can be obtained from the former (by letting  $t$  tend to infinity), a relatively simple mathematical procedure can be used if, at the outset, it is known that only the steady-state solution is required (see Annex A). If on the other hand a transient solution is required, then a much more specialised procedure involving, for

example, Laplace transforms or matrix algebra (see Annex C) may be needed. In general, reliability, availability, maintainability or safety measures can be derived from state probabilities.

The distinction between reliability, availability, maintainability and safety measures lies mainly in the focus of the analyzes and the interpretation of results. To explain this, a restorable element can be considered, whose performance is usually defined by a failure rate  $\lambda$  and a restoration rate  $\mu$ . Usually, after a failure within an item has appeared, at least two things have to occur in order to get the item working again:

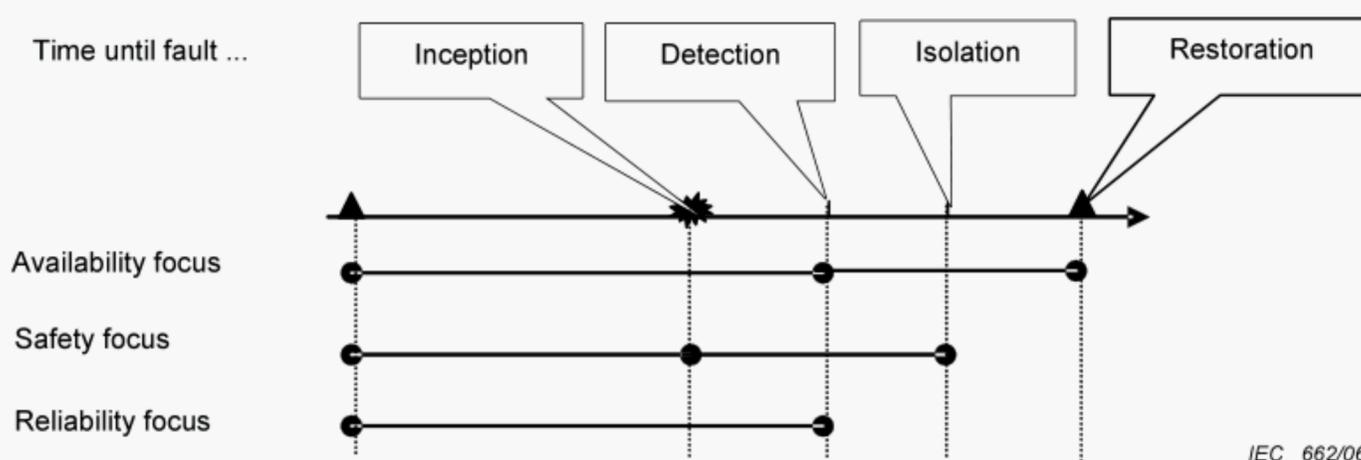
- the fault has to be detected and isolated (sometimes also called negated: this means that a state, where a failure has no further consequence, should be entered);
- the item has to be restored and put back into service.

The restoration time in this context includes the logistic time for restoration after fault detection, actual restoration time (fault finding, restoration, replacement, check) and time to put the elements or the system itself into operation.

In the common basic model, the four time intervals of interest need to be assigned to two parameters (a failure rate  $\lambda$  and a restoration rate  $\mu$ ) only.

In the context of reliability, maintainability or availability, the time to detection is taken into account by the failure rate calculation and the time from detection to restoration by the restoration rate calculation. Safety-critical applications may not rely on self-tests or similar measures (which are common in the availability context), but the detection and isolation has to be performed independently of the item (see IEC 61508 for particular requirements and examples). The distinction between reliability, maintainability and availability finally lies in the focus on different target measures, MTTF, MDT or  $A(t)$ .

In a safety context, generally the actual restoration time is neglected, if other control measures are taken during this period. In this case, the restoration rate calculation from reliability analysis accounts for the complete time to isolation. However, the interpretation may differ also in several applications, Figure 3 shows an example interpretation only.



**Figure 3 – Interpretation of failure and restoration times in different contexts**

However, the major observation is that while the model and the mathematics used may be the same, it is the interpretation of the parameters and of the results that make a major difference.

## 9.2 Evaluation of reliability measures

For reliability analyzes, all down states at system level in the state transition diagram are made absorbing. The probability that the system is in a given state at time  $t$  is calculated using special mathematical techniques (see Annexes A to C). As  $t$  tends to infinity, the

probability associated with each functioning state approaches zero, and the sum of the probabilities of absorbing states approaches unity.

One of the common reliability measures is MTTF. When evaluating the state transition diagram, the MTTF for the whole system is the mean of the total of the times spent by the system in up states before making a transition to an absorbing state. This mean time depends on the state of the system at  $t=0$ ;  $MTTF_{S_i}$  is used to specify this dependence (see Annex A).

### 9.3 Evaluation of availability and maintainability measures

For availability analysis, it must be verified that in the state transition diagram every state can be reached from every other state. The probability that the system is in a given state at time  $t$  is determined by the techniques given in Annexes A to C. The availability  $A(t)$  is equal to the sum of the state probabilities associated with the up states. 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,  $A$ .

Other useful measures such as the following can also be evaluated (see Annex A):

- failure intensity at system level;
- mean time spent in a given state  $i$ ;
- frequency of entering a given state  $i$ ;
- frequency of leaving a given state  $i$ .

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 the mean time spent in the up states and MDT the mean time spent in the down states.

### 9.4 Evaluation of safety measures

The evaluation of safety measures is basically similar to the evaluation of reliability or availability measures. The terminology is, however, different. In safety applications, the down states are further subdivided in safe down states (where the system is not up and not potentially hazardous) and dangerous down (or hazardous) states (where the system is potentially hazardous).

The purpose is, for example, to assess:

- the mean time to the first occurrence of a hazardous failure (MTTFH);
- the dangerous failure rate (DFR);
- the probability of failure on demand (PFD).

The MTTFH and DFR calculations are similar to those of the MTTF and the failure rate calculations, respectively. They are evaluated like the corresponding reliability measure but only with respect to dangerous down states. The PFD at time  $t$  is the probability that the system is in a hazardous state at time  $t$  and is evaluated like the unavailability at time  $t$ . Sometimes the average PFD up to time  $t$  is required, which can be obtained by integration as

$$PFD_{avg} = \frac{1}{t} \int_0^t PFD(s) ds .$$

## 10 Documentation of results

The reporting of the results of the analysis should incorporate the following elements:

- a) specification of the desired measures (e.g. reliability, availability, maintainability, safety);

- b) the main assumptions used, including justification (for instance, constant failure and restoration rates);
- c) justification, why Markov techniques are appropriate;
- d) description of the state transition diagram including in-depth examination of the following aspects:
  - identification of the up states and down states;
  - where applicable, the reasons why some states are grouped and others are omitted;
  - transitions between states;
  - the choice of numerical values for the transition rates;
  - underlying assumptions associated with the construction of the diagram;
- e) description of the
  - computation methods;
  - computer programs, if used;
- f) numerical results
  - results in numerical and graphical form;
  - influence of the assumptions used in constructing the state transition diagram or in calculations;
  - sensitivity analysis.

Also see IEC 60300-3-1.

## Annex A (informative)

### Basic mathematical relationships for Markov techniques

#### A.1 General

This annex deals with models based on time-homogeneous Markov processes with finitely many states and continuous time. Because of the memory-less property that characterizes such processes, the time spent in any given state is exponentially distributed. For reliability models, this implies that failure and restoration rates ( $\lambda$  and  $\mu$ ) of all elements in a system are constant (time independent). Failure and or restoration rates can change only at a state change.

#### A.2 Transition rates matrix

##### A.2.1 State transition diagram

A time-homogeneous Markov process is completely characterized by the transition rates matrix  $Q = [q_{ij}]$  and the initial probability vector at time  $t = 0$ . A useful visualization of the transition rates matrix is the state transition diagram. For setting up this diagram, a reliability block diagram (if it exists) and a FMEA for the system can be very useful. In any case, to reduce the number of states it is recommended to collect any group of  $n$  series elements ( $n = 2, 3, \dots$ ) in one element with failure rate  $\lambda_1 + \dots + \lambda_n$  and restoration rate  $(\lambda_1 + \dots + \lambda_n) / (\lambda_1 / \mu_1 + \dots + \lambda_n / \mu_n)$ , provided  $\lambda_i \ll \mu_i, i = 1, \dots, n$ .

Having drawn and verified the state transition diagram (taking care of retained failure modes, assumed restoration priority, and particularities specific to the system considered), the state space  $\{0, 1, \dots, m\}$  is divided into two complementary sets UP for the up states and D for the down states, where  $m$  is the total number of states. The set of down states can vary according to the system aspect being evaluated (reliability or safety).

##### A.2.2 Basic relations useful in evaluating Markov techniques

**A.2.2.1** For reliability evaluation, the mean time to system failure  $MTTF_{S_i}$  when starting with system in state  $i$  at  $t = 0$ , is obtained by solving

$$MTTF_{S_i} = \frac{1}{q_i} + \sum_{\substack{j \in UP \\ j \neq i}} \frac{q_{ij}}{q_i} MTTF_{S_j}, \quad i \in UP, \quad q_i = \sum_{\substack{j=0 \\ j \neq i}}^m q_{ij}$$

NOTE 1 The above system of algebraic equations can also be used to compute the mean time to a dangerous failure (for safety investigations) by defining adequately the set UP of up states.

NOTE 2 The exact expression for the reliability function  $R_{S_i}(t)$ , when starting with system in state  $i$  at  $t = 0$ , is given by solving (e.g. using Laplace transforms).

$$R_{S_i}(t) = e^{-q_i t} + \sum_{\substack{j \in UP \\ j \neq i}} \int_0^t q_{ij} e^{-q_i x} R_{S_j}(t-x) dx, \quad i \in UP$$

**A.2.2.2** The asymptotic and steady-state availability  $A_S$  is given by

$$A_S = \sum_{j \in UP} P_j$$

with  $P_j$  as solution of

$$P_j = \sum_{\substack{i=0 \\ i \neq j}}^m P_i \frac{q_{ij}}{q_j}, \quad j = 0, \dots, m, \quad P_j > 0, \quad \sum_{j=0}^m P_j = 1, \quad q_i = \sum_{\substack{j=0 \\ j \neq i}}^m q_{ij}$$

Since these equations are not independent, one equation for  $P_j$  (arbitrarily chosen) must be dropped and replaced by

$$\sum_{j=0}^m P_j = 1$$

**A.2.2.3** Since the failure rate is assumed constant, a good approximation for the interval reliability  $IR_S$  in steady-state is

$$IR_S(t, t + \theta) = \sum_{j \in UP} P_j R_{S_j}(\theta) \approx A_S e^{-\theta / MTTFS_0}$$

Where 0 denotes the state in which all elements are operating (or ready to operate).

**A.2.2.4** The asymptotic and steady-state failure intensity (failure frequency) at system level  $z_S$  is given by

$$z_S = \sum_{\substack{j \in UP \\ i \in D}} P_j q_{ji} = \sum_{j \in UP} P_j \left( \sum_{i \in D} q_{ji} \right)$$

NOTE 1 In the above equation, all transition rates  $q_{ji}$  leaving state  $j \in UP$  toward  $i \in D$  have to be considered.

NOTE 2 For small  $\Delta t$ ,  $z_S \Delta t$  gives the probability for a transition from a state in the set of up states to a state in the set of down states, and vice versa, within  $(t, t + \Delta t)$  for any arbitrary time  $t$  (steady-state).

**A.2.2.5** The  $MUT_S$  (mean up time at system level) and the  $MDT_S$  (mean down time at system level) are given in steady-state by

$$MUT_S = \frac{A_S}{z_S} \quad \text{and} \quad MDT_S = \frac{1 - A_S}{z_S}$$

NOTE  $MUT_S + MDT_S = 1/z_S$ , where  $z_S$  is the asymptotic and steady-state failure intensity (failure frequency) at system level given in A.2.2.4.

**A.2.2.6** For a given state  $i$ , it holds in particular that

$\frac{1}{q_i}$  = unconditional mean time spent in state  $i$

$P_i(t)q_i$  = frequency of a transition out of state  $i$

$$\sum_{\substack{j=0 \\ j \neq i}}^m P_j(t) q_{ji} \Delta t = \text{unconditional probability of entering state } i \text{ within } (t, t + \Delta t) \text{ for } \Delta t \text{ small}$$

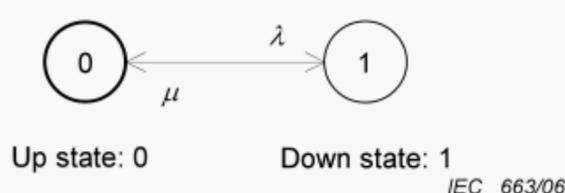
For large series/parallel structures, approximate expressions are known in the literature. For very large or complex systems, a Monte Carlo simulation can become necessary.

## Annex B (informative)

### Example: Development of state transition diagrams

#### B.1 One-element system

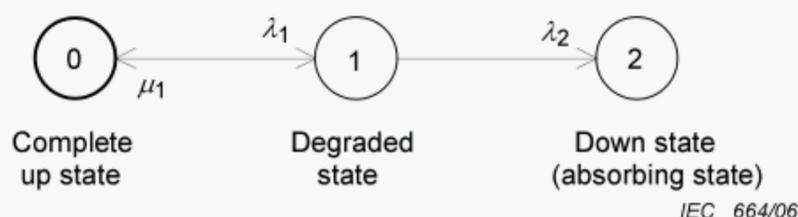
The first step, in applying the Markov technique, is to define the system states. As an example, consider a one-element system. For the simplest case, the corresponding state transition diagram comprises only two states: an up state 0, with transition rate  $\lambda$ , and a down state 1, with transition rate  $\mu$ , as shown in Figure B.1.



**Figure B.1 – State transition diagram for a restorable one-element system**

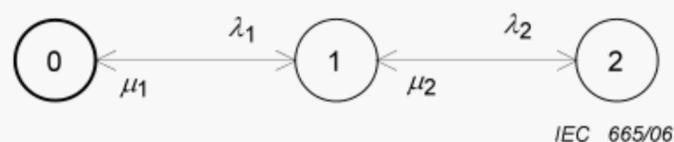
The arrow from state 0 to state 1 denotes a failure occurrence with the probability  $\lambda\Delta t$  in the small time interval  $(t, t+\Delta t)$  given that the element was in state 0 at  $t$ . Similarly, the arrow from state 1 to state 0 shows completion of a system restoration with the probability  $\mu\Delta t$ .

A one-element system can also be modelled using more than the two states 0 (functional) and 1 (failed). A degraded state which is still an up state may also be included. Such a state is state 1 in Figure B.2: the system failure state being state 2 (assuming no repair is possible in state 2).



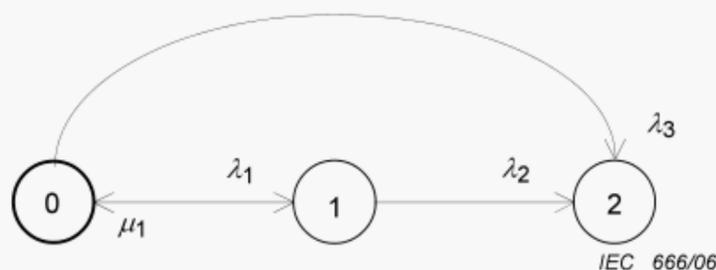
**Figure B.2 – State transition diagram with three states for a one-element system**

If restoration can be carried out from state 2, the system can be modelled by the diagram in Figure B.3 where the restoration rate  $\mu_2$  represents the transition from state 2 to state 1.



**Figure B.3 – State transition diagram when restorations may be made from state 2 for a one-element system**

In many cases a direct catastrophic failure path from state 0 to state 2 has to be considered and an arrow  $\lambda_3$ , is added to Figure B.2 to give Figure B.4.



**Figure B.4 – State transition diagram when direct transition is considered for a one-element system**

The model depicted in Figure B.1 can be used to get the instantaneous availability  $A(t)$  and the steady-state availability  $A$ . If calculation of reliability  $R(t)$  is required, the state transition diagram shown in Figure B.5 is applicable. In this case, only the failure rate  $\lambda$  is considered and state 1 becomes an absorbing state.

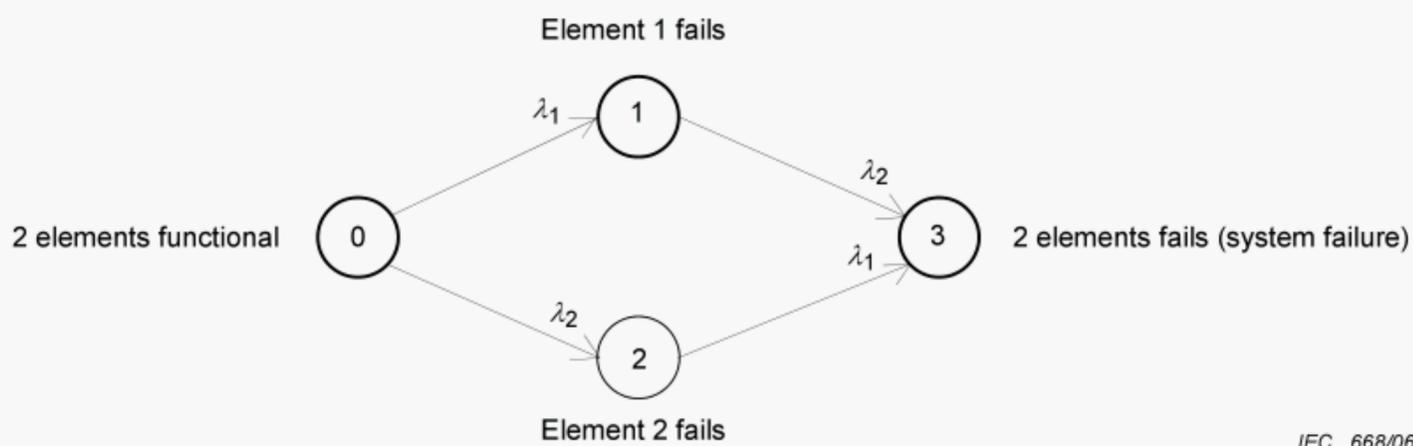


**Figure B.5 – State transition diagram for the evaluation of reliability of a one-element system**

## B.2 Two-element system

Basically, since an element can be represented by two states 0 (up) and 1 (down), possible system states for a system with two independent elements are (0 0), (0 1), (1 0), (1 1). If the two-element system is a series system, (0 0) is the only up state and (0 1), (1 0), (1 1) are down states. If the system contains active or stand-by redundancy, (0 0), (0 1), (1 0) are all up states. In what follows, consideration will be given solely to a 1-out-of-2 active redundant system.

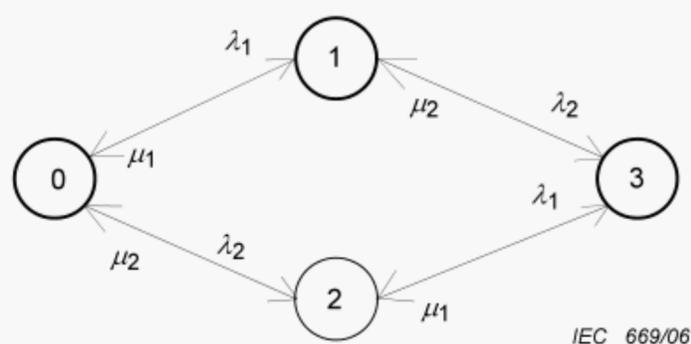
The state transition diagram for a 1-out-of-2 active redundant system with no restorable elements is given in Figure B.6.



NOTE The state symbols may also be marked (0 0), (0 1), (1 0), (1 1) corresponding to states 0,1,2,3 respectively.

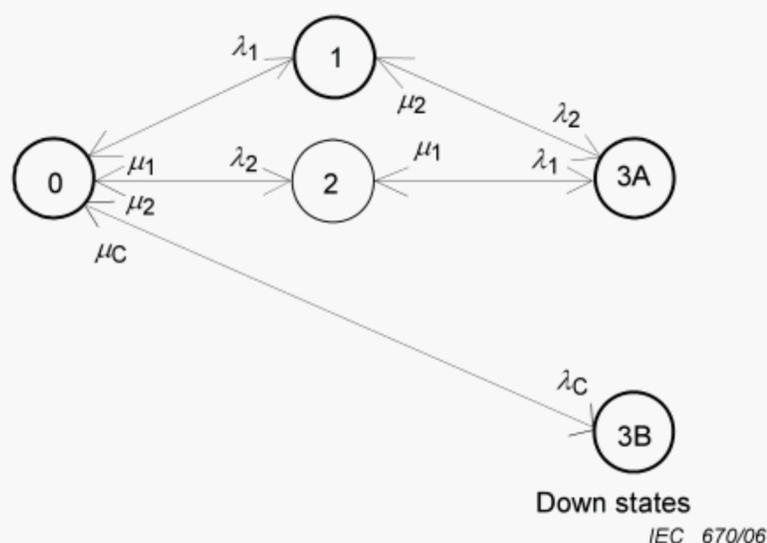
**Figure B.6 – State transition diagram for a 1-out-of-2 active redundant system with no restorable elements**

If the system is restorable, arrows are added representing restoration with rates  $\mu_i$  ( $i=1,2$ ) as illustrated in Figure B.7. Note that no resource limitation for restoration is assumed here (from state 3).



**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**

If a common cause failure disables simultaneously both elements in a restorable 1-out-of-2 redundant 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 elements. This has to be taken into account as shown in Figure B.8, where  $\lambda_C$  and  $\mu_C$  denote the common cause failure and restoration rates, respectively.



**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**

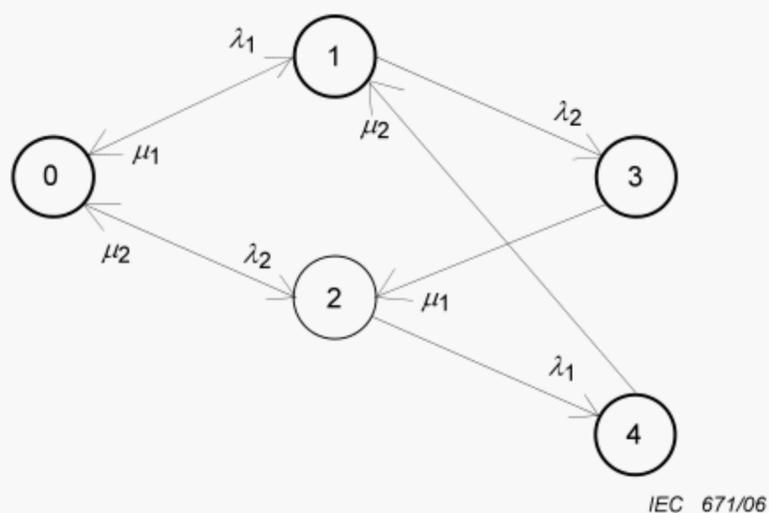
As an example, consider a system with two stand-by generators which would not start at low ambient temperatures. When the system reaches the state "both generators failed to start", the restoration time will depend on whether each generator was disabled by an independent mechanical failure, or both generators were incapacitated by a common cause, such as low ambient temperature. Therefore, the state "both generators failed to start due to independent faults" has to 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. Therefore, both states form a combined state from which the reliability, availability, maintainability and safety measures can be obtained

State transition diagrams can take maintenance strategies into account, but particular care has to be taken with respect to the memory-less property. Assume that only one restoration team exists and that the maintenance strategy is as follows: the restoration priority is for the component which has failed first. The order of failure occurrences has to be taken into account. This is illustrated by the state transition diagram of Figure B.9.

In Figure B.9 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.

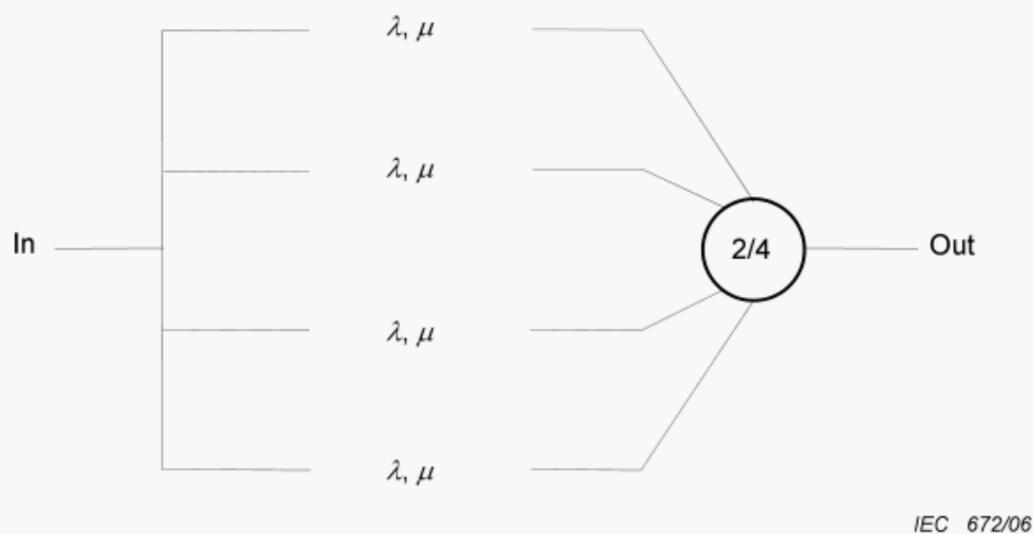
Note that in the state transition diagram depicted in Figure B.9, the mean time to repair a component, e.g. component 1, actually takes longer than the intended MTTR  $1/\mu_1$ . If in state 1 a second failure occurs, the repair time up to the second failure is not taken into account after transition to state 3, where the repair of component 1 starts again, due to the memory-less property. In order to compensate for the overrepresentation of the repair time, it would be possible to increase the residual repair rates. In the particular case in Figure B.9, the repair rates in states 3 and 4 would have to be doubled as a compensation. For other levels of redundancy and non-instantaneous repair, the compensation would be different and more difficult to apply.



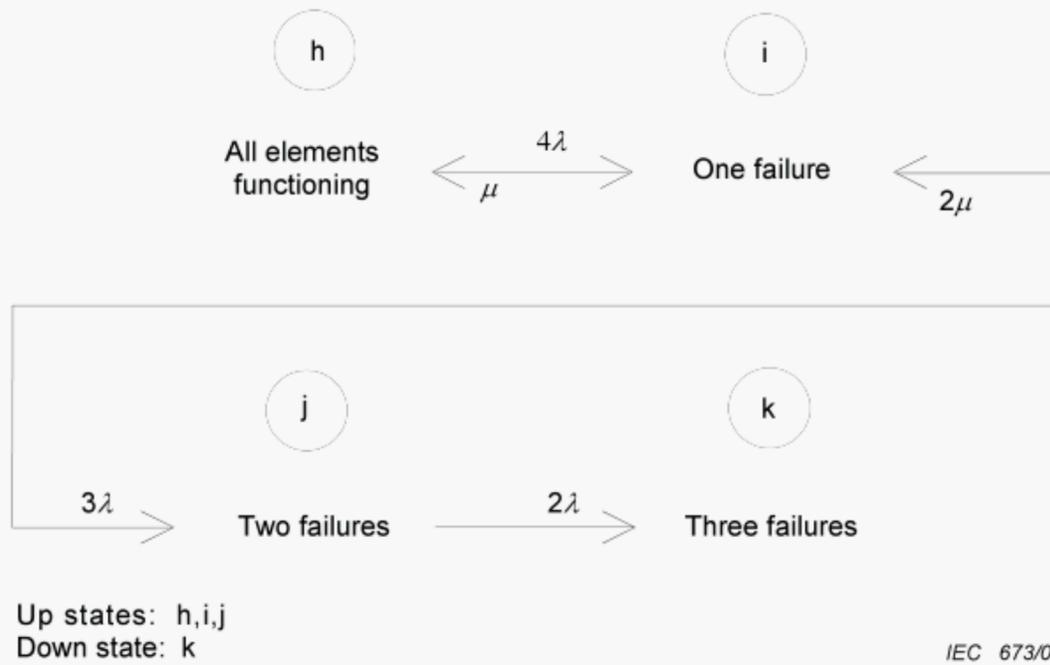
**Figure B.9 – State transition diagram for a 1-out-of-2 active redundant system with only one restoration team and restoration priority as first-in/first-out**

### B.3 Aggregation of state transition diagram

For ease of computation, attempts should be made to construct state transition diagrams using a number of states as small as possible. If elements in a parallel redundant configuration are assumed to be independent and have the same failure rate  $\lambda$ , and the same restoration rate  $\mu$  as shown in Figure B.10 for a 2-out-of-4 active redundant system, then the state transition diagram can be expressed in an aggregated form illustrated by Figure B.11. In Figure B.11, it is assumed that unlimited repair resources are available. Note that once three elements are failed, the system is failed and no further failure is considered.



**Figure B.10 – Reliability block diagram for a 2-out-of-4 active redundant system**



**Figure B.11 – Aggregated state transition diagram for reliability computation of the system in Figure B.10**

From the above diagram, a set of algebraic equations can be obtained and solved (see Annex A) to give the following expression for the system mean time to failure when starting in state 0 (all 4 elements up) at  $t=0$  ( $MTTF_{S0}$ ):

$$\begin{aligned}
 MTTF_{S0} &= \frac{1}{4\lambda} \left( \frac{\mu}{3\lambda} \cdot \frac{2\mu}{2\lambda} + \frac{\mu}{3\lambda} + 1 \right) \\
 &\quad + \frac{1}{3\lambda} \left( \frac{2\mu}{2\lambda} + 1 \right) \\
 &\quad + \frac{1}{2\lambda}
 \end{aligned}$$

## Annex C (informative)

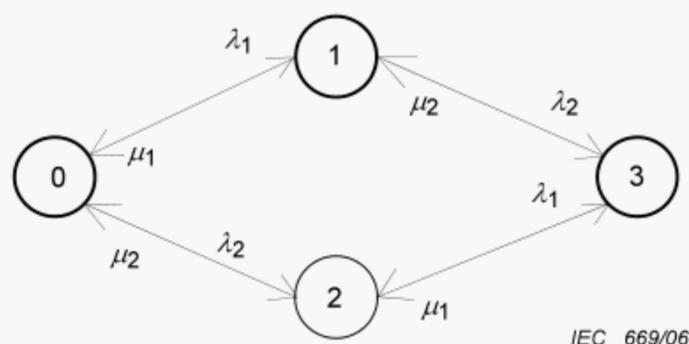
### Example: Numerical evaluation of some reliability, availability, maintainability and safety measures for a 1-out-of-2 active redundant system

#### C.1 Objective

In this annex, a 1-out-of-2 restorable active redundant system with no restoration constraints considered. The measures to be assessed are instantaneous availability, asymptotic availability, reliability and MTTF. Conventional mathematical methods commonly used in such evaluations are applied.

#### C.2 Modelling

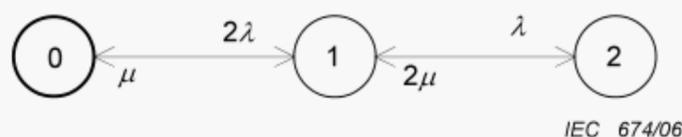
The state transition diagram for the 1-out-of-2 active redundant system is given in Figure C.1 for the assessment of the availability. State 3 is the down state.



**Figure C.1 – State transition diagram for 1-out-of-2 active redundant system with different elements and two restoration teams**

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.

Assuming that the two elements in the system are identical or have the same failure and restoration rates, the reduced diagram then becomes as Figure C.2.



**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**

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.

### C.3 Differential equation method

#### C.3.1 Method for evaluating 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 C.2). The following differential equations are obtained from the state transition diagram of Figure C.2:

$$\begin{aligned}\frac{dP_0(t)}{dt} &= -2\lambda P_0(t) + \mu P_1(t) \\ \frac{dP_1(t)}{dt} &= 2\lambda P_0(t) - (\lambda + \mu)P_1(t) + 2\mu P_2(t) \\ \frac{dP_2(t)}{dt} &= \lambda P_1(t) - 2\mu P_2(t)\end{aligned}$$

Thus the transition rates matrix, which can also be directly established from the state transition diagram, becomes

$$Q(\lambda, \mu) = \begin{bmatrix} -2\lambda & 2\lambda & 0 \\ \mu & -(\lambda + \mu) & \lambda \\ 0 & 2\mu & -2\mu \end{bmatrix}$$

and we can formally express the differential equation as  $\frac{d}{dt}P(t) = Q(\lambda, \mu)^T \times P(t)$ , where

$$P(t) = [P_0(t) \ P_1(t) \ P_2(t)]^T.$$

It is now necessary to find the eigenvalues  $\varepsilon(\lambda, \mu)$  and eigenvectors  $E(\lambda, \mu)$  of the matrix  $Q^T$ . In the case of distinct eigenvalues (which in continuous-time Markov techniques holds for most models of interest for almost all parameter values) the vector of state probabilities can directly be expressed by

$$P(t) = E(\lambda, \mu) \times \begin{bmatrix} \exp(\varepsilon(\lambda, \mu)_0 t) & & \\ & \exp(\varepsilon(\lambda, \mu)_1 t) & \\ & & \exp(\varepsilon(\lambda, \mu)_2 t) \end{bmatrix} \times E(\lambda, \mu)^{-1} \times P(0)$$

By evaluating the above matrix equation, 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, i.e.

$$P(0) = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

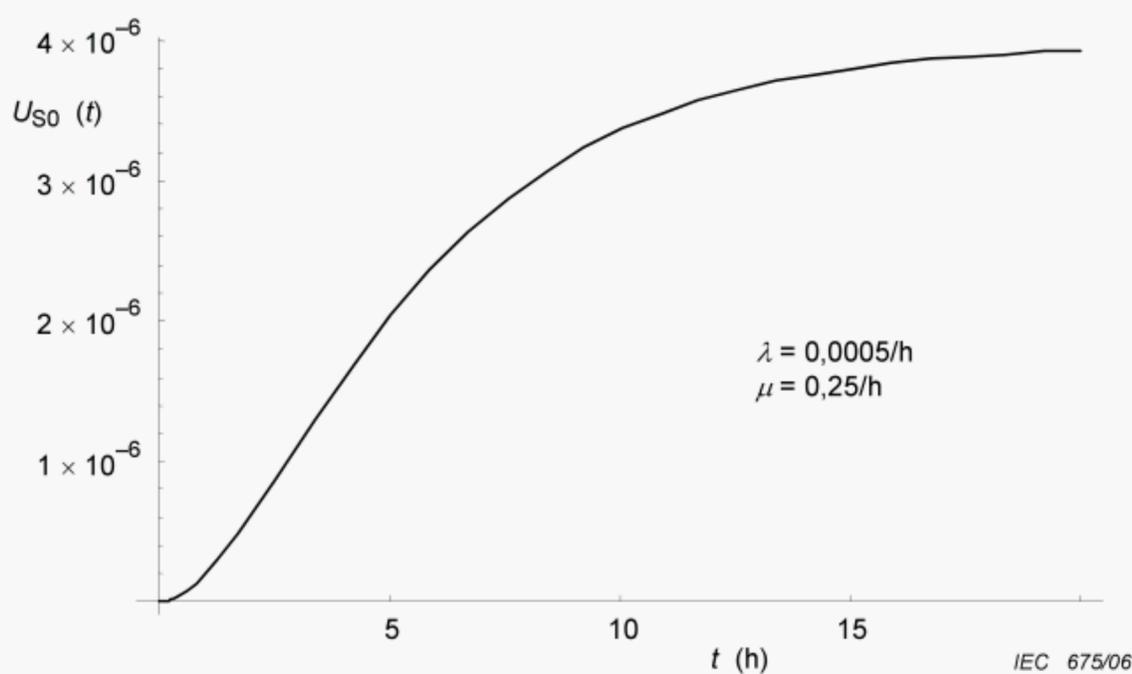
The instantaneous availability,  $A_{S0}(t)$  is then computed as

$$A_{S0}(t) = P_0(t) + P_1(t)$$

The indices  $S0$  in  $A_{S0}(t)$  make clear that one deals with the availability at system level for the system starting in state 0 at  $t=0$ . For this simple model, an explicit expression in  $\lambda$  and  $\mu$  can be calculated by e. g. using Laplace transforms and is given by

$$A_{S0}(t) = \frac{\mu^2 + 2\lambda\mu}{(\lambda + \mu)^2} + \left(\frac{\lambda}{\lambda + \mu}\right)^2 e^{-(\lambda+\mu)t} (2 - e^{-(\lambda+\mu)t})$$

Figure C.3 shows a numerical example for the unavailability  $U_{S0}(t) = 1 - A_{S0}(t)$ .



**Figure C.3 – Numerical example for unavailability**

In the general case, the differential equations would have to be evaluated by use of a mathematical computer program either numerically or in a symbolic form.

From  $A_{S0}(t)$ , the asymptotic and steady-state availability  $A_{S0}(\infty) = A_S$  follows immediately. Alternatively, setting  $P_{i(\infty)} = P_i$  ( $i = 0, 1, 2$ ) for the asymptotic and steady-state value of the state probabilities,  $A_S$  follows as  $A_S = P_0 + P_1$  with  $P_i$  as solution of the following equations (see Annex A)

$$\begin{aligned} 0 &= -2\lambda P_0 + \mu P_1 \\ 0 &= 2\lambda P_0 - (\lambda + \mu)P_1 + 2\mu P_2 \\ 0 &= \lambda P_1 - 2\mu P_2 \end{aligned}$$

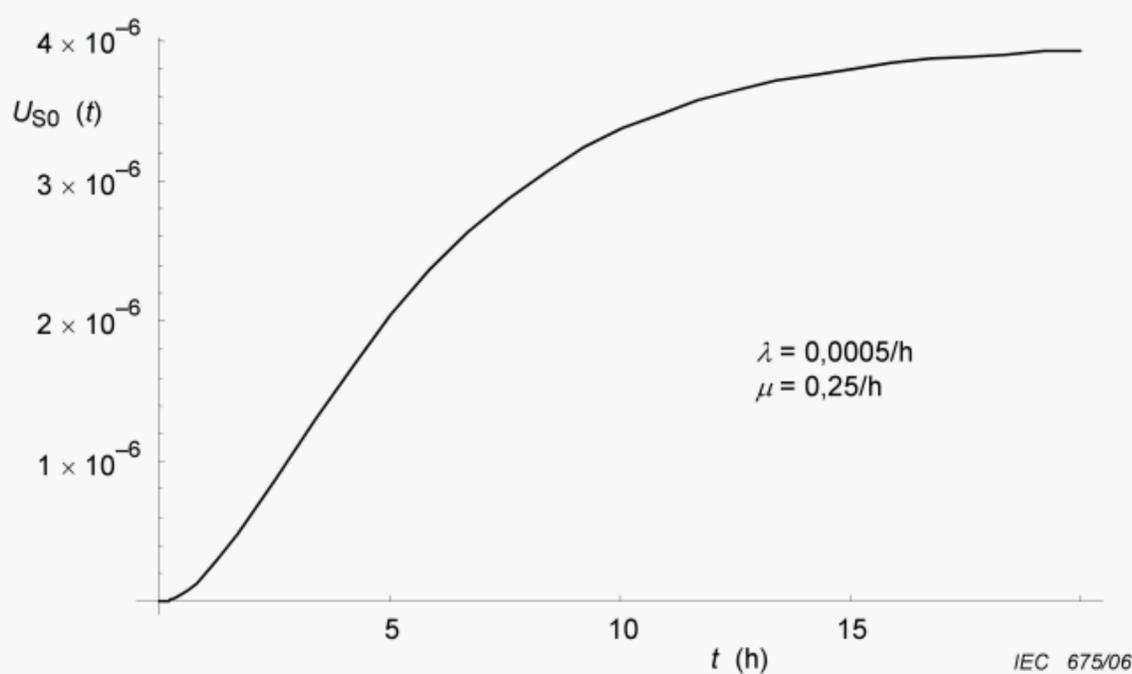
In the above set of algebraic equations, any one can be obtained from the other two, so that there are really only two useful equations and three unknowns. To overcome this difficulty, the fact that  $P_0 + P_1 + P_2 = 1$  is used as the third equation. Hence, after some mathematical manipulation, it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

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

The indices  $S0$  in  $A_{S0}(t)$  make clear that one deals with the availability at system level for the system starting in state 0 at  $t=0$ . For this simple model, an explicit expression in  $\lambda$  and  $\mu$  can be calculated by e. g. using Laplace transforms and is given by

$$A_{S0}(t) = \frac{\mu^2 + 2\lambda\mu}{(\lambda + \mu)^2} + \left(\frac{\lambda}{\lambda + \mu}\right)^2 e^{-(\lambda+\mu)t} (2 - e^{-(\lambda+\mu)t})$$

Figure C.3 shows a numerical example for the unavailability  $U_{S0}(t) = 1 - A_{S0}(t)$ .



**Figure C.3 – Numerical example for unavailability**

In the general case, the differential equations would have to be evaluated by use of a mathematical computer program either numerically or in a symbolic form.

From  $A_{S0}(t)$ , the asymptotic and steady-state availability  $A_{S0}(\infty) = A_S$  follows immediately. Alternatively, setting  $P_{i(\infty)} = P_i$  ( $i = 0, 1, 2$ ) for the asymptotic and steady-state value of the state probabilities,  $A_S$  follows as  $A_S = P_0 + P_1$  with  $P_i$  as solution of the following equations (see Annex A)

$$\begin{aligned} 0 &= -2\lambda P_0 + \mu P_1 \\ 0 &= 2\lambda P_0 - (\lambda + \mu)P_1 + 2\mu P_2 \\ 0 &= \lambda P_1 - 2\mu P_2 \end{aligned}$$

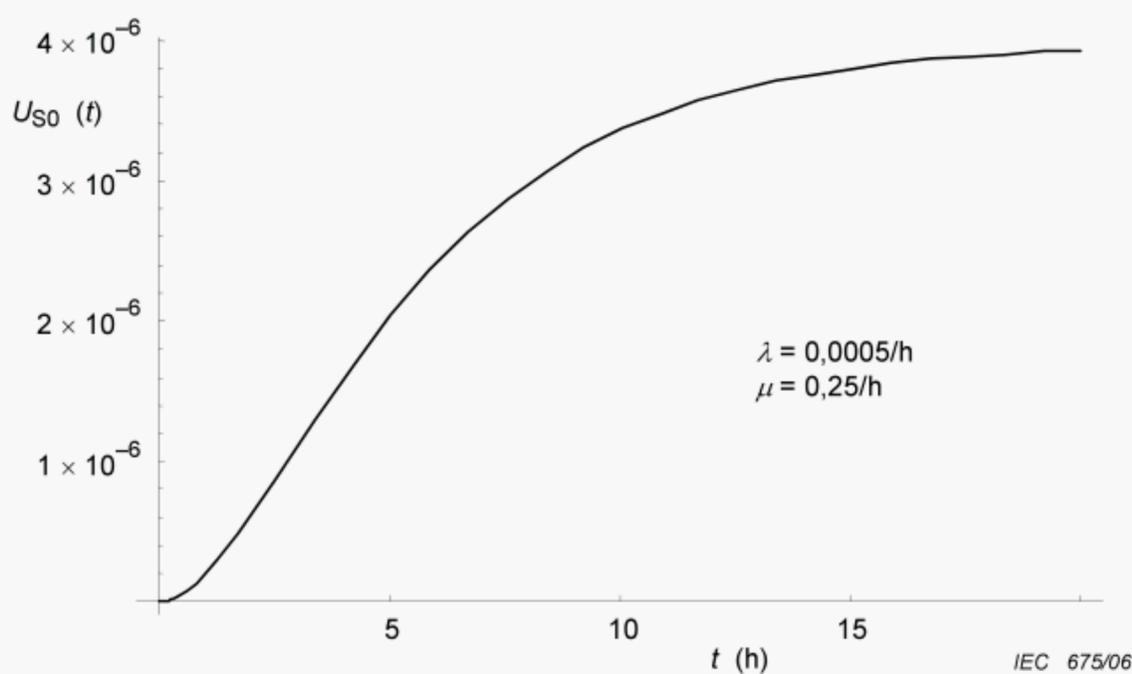
In the above set of algebraic equations, any one can be obtained from the other two, so that there are really only two useful equations and three unknowns. To overcome this difficulty, the fact that  $P_0 + P_1 + P_2 = 1$  is used as the third equation. Hence, after some mathematical manipulation, it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

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

The indices  $S0$  in  $A_{S0}(t)$  make clear that one deals with the availability at system level for the system starting in state 0 at  $t=0$ . For this simple model, an explicit expression in  $\lambda$  and  $\mu$  can be calculated by e. g. using Laplace transforms and is given by

$$A_{S0}(t) = \frac{\mu^2 + 2\lambda\mu}{(\lambda + \mu)^2} + \left(\frac{\lambda}{\lambda + \mu}\right)^2 e^{-(\lambda+\mu)t} (2 - e^{-(\lambda+\mu)t})$$

Figure C.3 shows a numerical example for the unavailability  $U_{S0}(t) = 1 - A_{S0}(t)$ .



**Figure C.3 – Numerical example for unavailability**

In the general case, the differential equations would have to be evaluated by use of a mathematical computer program either numerically or in a symbolic form.

From  $A_{S0}(t)$ , the asymptotic and steady-state availability  $A_{S0}(\infty) = A_S$  follows immediately. Alternatively, setting  $P_{i(\infty)} = P_i$  ( $i = 0, 1, 2$ ) for the asymptotic and steady-state value of the state probabilities,  $A_S$  follows as  $A_S = P_0 + P_1$  with  $P_i$  as solution of the following equations (see Annex A)

$$\begin{aligned} 0 &= -2\lambda P_0 + \mu P_1 \\ 0 &= 2\lambda P_0 - (\lambda + \mu)P_1 + 2\mu P_2 \\ 0 &= \lambda P_1 - 2\mu P_2 \end{aligned}$$

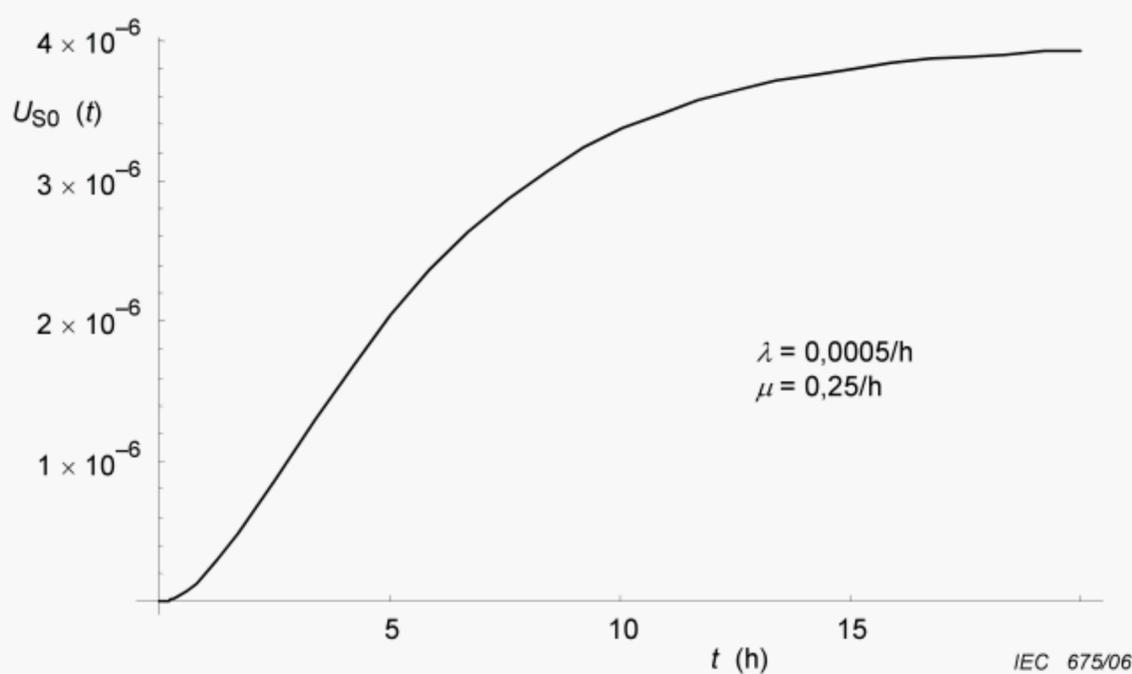
In the above set of algebraic equations, any one can be obtained from the other two, so that there are really only two useful equations and three unknowns. To overcome this difficulty, the fact that  $P_0 + P_1 + P_2 = 1$  is used as the third equation. Hence, after some mathematical manipulation, it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

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

The indices  $S0$  in  $A_{S0}(t)$  make clear that one deals with the availability at system level for the system starting in state 0 at  $t=0$ . For this simple model, an explicit expression in  $\lambda$  and  $\mu$  can be calculated by e. g. using Laplace transforms and is given by

$$A_{S0}(t) = \frac{\mu^2 + 2\lambda\mu}{(\lambda + \mu)^2} + \left(\frac{\lambda}{\lambda + \mu}\right)^2 e^{-(\lambda+\mu)t} (2 - e^{-(\lambda+\mu)t})$$

Figure C.3 shows a numerical example for the unavailability  $U_{S0}(t) = 1 - A_{S0}(t)$ .



**Figure C.3 – Numerical example for unavailability**

In the general case, the differential equations would have to be evaluated by use of a mathematical computer program either numerically or in a symbolic form.

From  $A_{S0}(t)$ , the asymptotic and steady-state availability  $A_{S0}(\infty) = A_S$  follows immediately. Alternatively, setting  $P_{i(\infty)} = P_i$  ( $i = 0, 1, 2$ ) for the asymptotic and steady-state value of the state probabilities,  $A_S$  follows as  $A_S = P_0 + P_1$  with  $P_i$  as solution of the following equations (see Annex A)

$$\begin{aligned} 0 &= -2\lambda P_0 + \mu P_1 \\ 0 &= 2\lambda P_0 - (\lambda + \mu)P_1 + 2\mu P_2 \\ 0 &= \lambda P_1 - 2\mu P_2 \end{aligned}$$

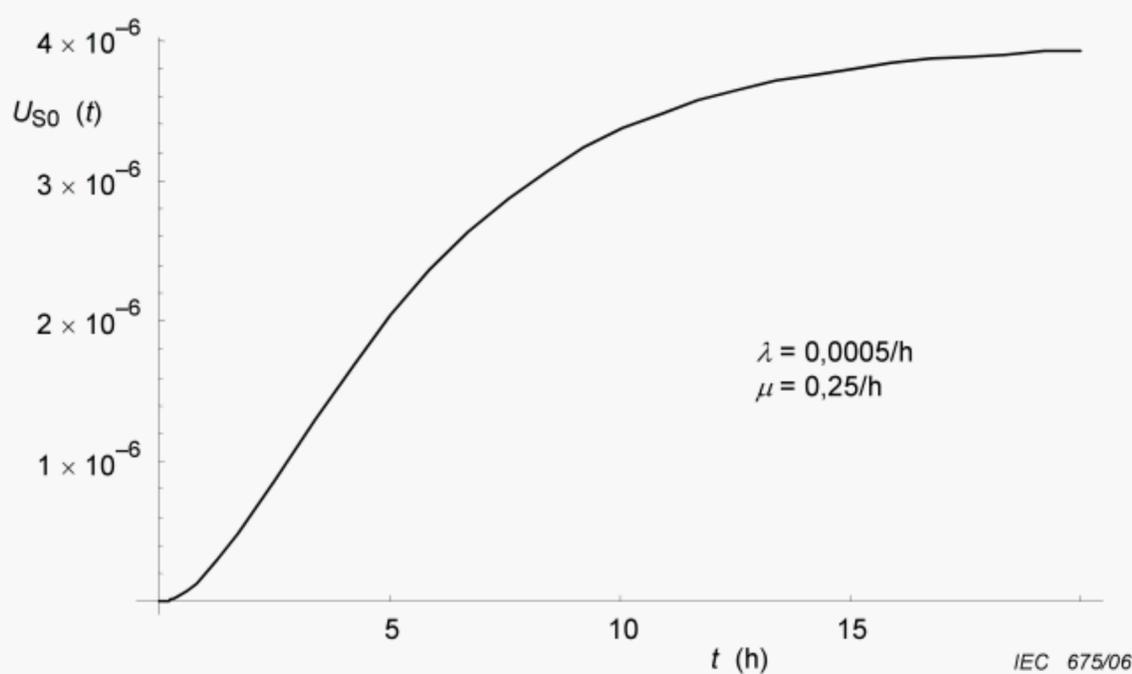
In the above set of algebraic equations, any one can be obtained from the other two, so that there are really only two useful equations and three unknowns. To overcome this difficulty, the fact that  $P_0 + P_1 + P_2 = 1$  is used as the third equation. Hence, after some mathematical manipulation, it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

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

The indices  $S0$  in  $A_{S0}(t)$  make clear that one deals with the availability at system level for the system starting in state 0 at  $t=0$ . For this simple model, an explicit expression in  $\lambda$  and  $\mu$  can be calculated by e. g. using Laplace transforms and is given by

$$A_{S0}(t) = \frac{\mu^2 + 2\lambda\mu}{(\lambda + \mu)^2} + \left(\frac{\lambda}{\lambda + \mu}\right)^2 e^{-(\lambda+\mu)t} (2 - e^{-(\lambda+\mu)t})$$

Figure C.3 shows a numerical example for the unavailability  $U_{S0}(t) = 1 - A_{S0}(t)$ .



**Figure C.3 – Numerical example for unavailability**

In the general case, the differential equations would have to be evaluated by use of a mathematical computer program either numerically or in a symbolic form.

From  $A_{S0}(t)$ , the asymptotic and steady-state availability  $A_{S0}(\infty) = A_S$  follows immediately. Alternatively, setting  $P_{i(\infty)} = P_i$  ( $i = 0, 1, 2$ ) for the asymptotic and steady-state value of the state probabilities,  $A_S$  follows as  $A_S = P_0 + P_1$  with  $P_i$  as solution of the following equations (see Annex A)

$$\begin{aligned} 0 &= -2\lambda P_0 + \mu P_1 \\ 0 &= 2\lambda P_0 - (\lambda + \mu)P_1 + 2\mu P_2 \\ 0 &= \lambda P_1 - 2\mu P_2 \end{aligned}$$

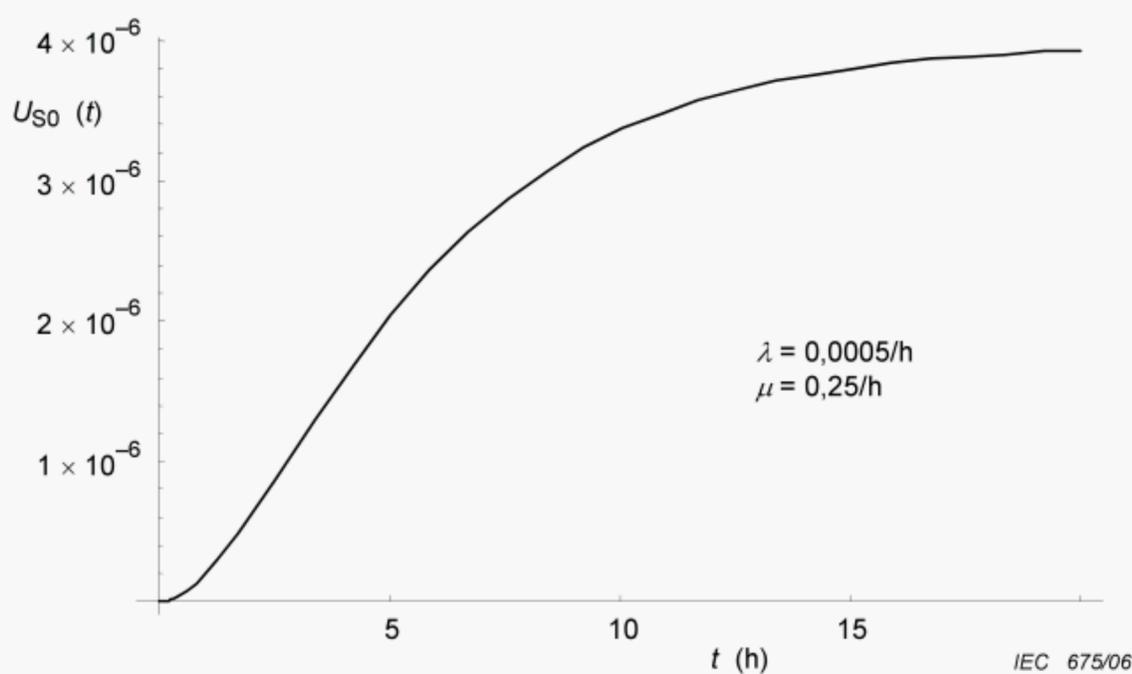
In the above set of algebraic equations, any one can be obtained from the other two, so that there are really only two useful equations and three unknowns. To overcome this difficulty, the fact that  $P_0 + P_1 + P_2 = 1$  is used as the third equation. Hence, after some mathematical manipulation, it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

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

The indices  $S0$  in  $A_{S0}(t)$  make clear that one deals with the availability at system level for the system starting in state 0 at  $t=0$ . For this simple model, an explicit expression in  $\lambda$  and  $\mu$  can be calculated by e. g. using Laplace transforms and is given by

$$A_{S0}(t) = \frac{\mu^2 + 2\lambda\mu}{(\lambda + \mu)^2} + \left( \frac{\lambda}{\lambda + \mu} \right)^2 e^{-(\lambda + \mu)t} (2 - e^{-(\lambda + \mu)t})$$

Figure C.3 shows a numerical example for the unavailability  $U_{S0}(t) = 1 - A_{S0}(t)$ .



**Figure C.3 – Numerical example for unavailability**

In the general case, the differential equations would have to be evaluated by use of a mathematical computer program either numerically or in a symbolic form.

From  $A_{S0}(t)$ , the asymptotic and steady-state availability  $A_{S0}(\infty) = A_S$  follows immediately. Alternatively, setting  $P_{i(\infty)} = P_i$  ( $i = 0, 1, 2$ ) for the asymptotic and steady-state value of the state probabilities,  $A_S$  follows as  $A_S = P_0 + P_1$  with  $P_i$  as solution of the following equations (see Annex A)

$$\begin{aligned} 0 &= -2\lambda P_0 + \mu P_1 \\ 0 &= 2\lambda P_0 - (\lambda + \mu)P_1 + 2\mu P_2 \\ 0 &= \lambda P_1 - 2\mu P_2 \end{aligned}$$

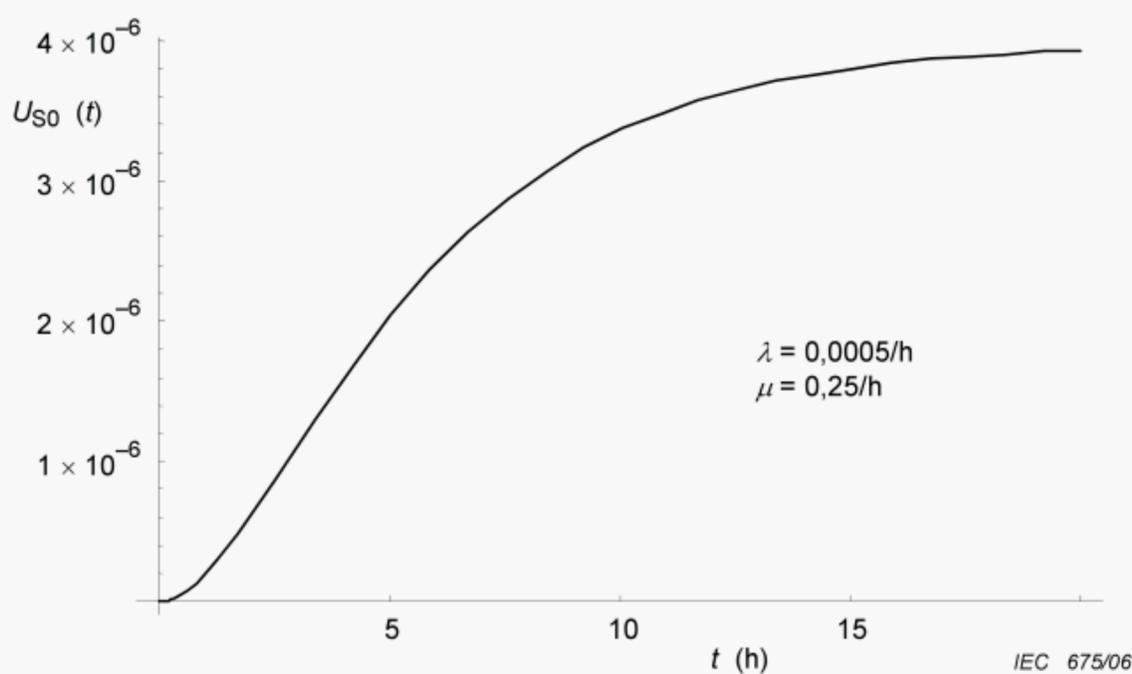
In the above set of algebraic equations, any one can be obtained from the other two, so that there are really only two useful equations and three unknowns. To overcome this difficulty, the fact that  $P_0 + P_1 + P_2 = 1$  is used as the third equation. Hence, after some mathematical manipulation, it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

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

The indices  $S0$  in  $A_{S0}(t)$  make clear that one deals with the availability at system level for the system starting in state 0 at  $t=0$ . For this simple model, an explicit expression in  $\lambda$  and  $\mu$  can be calculated by e. g. using Laplace transforms and is given by

$$A_{S0}(t) = \frac{\mu^2 + 2\lambda\mu}{(\lambda + \mu)^2} + \left(\frac{\lambda}{\lambda + \mu}\right)^2 e^{-(\lambda+\mu)t} (2 - e^{-(\lambda+\mu)t})$$

Figure C.3 shows a numerical example for the unavailability  $U_{S0}(t) = 1 - A_{S0}(t)$ .



**Figure C.3 – Numerical example for unavailability**

In the general case, the differential equations would have to be evaluated by use of a mathematical computer program either numerically or in a symbolic form.

From  $A_{S0}(t)$ , the asymptotic and steady-state availability  $A_{S0}(\infty) = A_S$  follows immediately. Alternatively, setting  $P_{i(\infty)} = P_i$  ( $i = 0, 1, 2$ ) for the asymptotic and steady-state value of the state probabilities,  $A_S$  follows as  $A_S = P_0 + P_1$  with  $P_i$  as solution of the following equations (see Annex A)

$$\begin{aligned} 0 &= -2\lambda P_0 + \mu P_1 \\ 0 &= 2\lambda P_0 - (\lambda + \mu)P_1 + 2\mu P_2 \\ 0 &= \lambda P_1 - 2\mu P_2 \end{aligned}$$

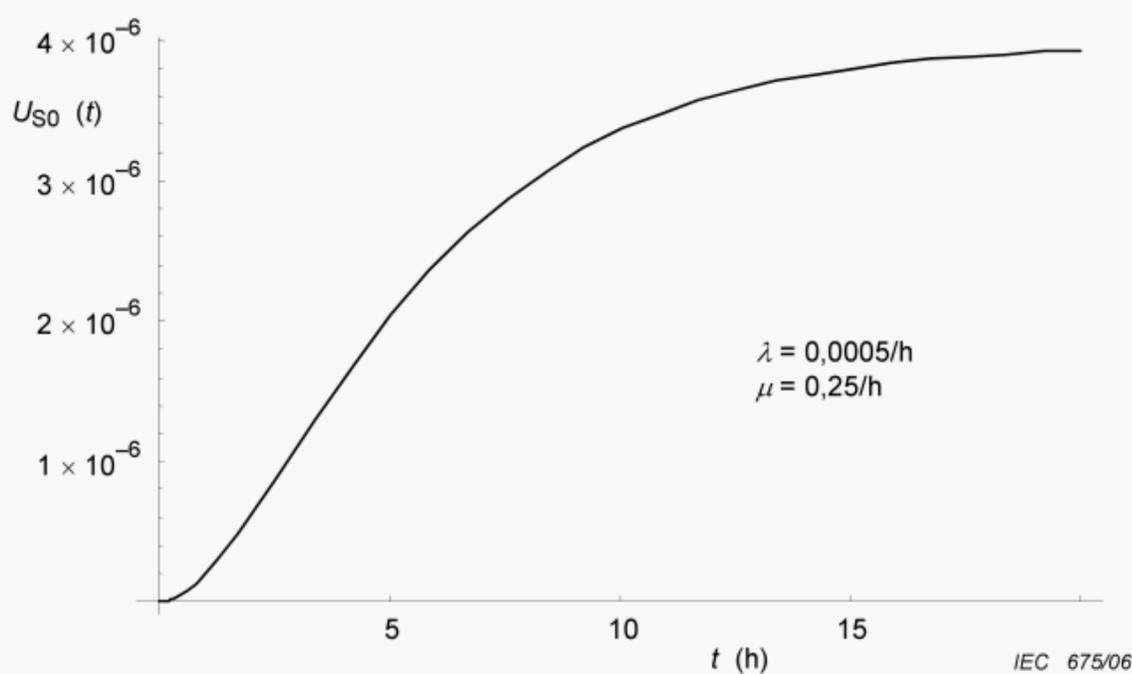
In the above set of algebraic equations, any one can be obtained from the other two, so that there are really only two useful equations and three unknowns. To overcome this difficulty, the fact that  $P_0 + P_1 + P_2 = 1$  is used as the third equation. Hence, after some mathematical manipulation, it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

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

The indices  $S0$  in  $A_{S0}(t)$  make clear that one deals with the availability at system level for the system starting in state 0 at  $t=0$ . For this simple model, an explicit expression in  $\lambda$  and  $\mu$  can be calculated by e. g. using Laplace transforms and is given by

$$A_{S0}(t) = \frac{\mu^2 + 2\lambda\mu}{(\lambda + \mu)^2} + \left( \frac{\lambda}{\lambda + \mu} \right)^2 e^{-(\lambda+\mu)t} (2 - e^{-(\lambda+\mu)t})$$

Figure C.3 shows a numerical example for the unavailability  $U_{S0}(t) = 1 - A_{S0}(t)$ .



**Figure C.3 – Numerical example for unavailability**

In the general case, the differential equations would have to be evaluated by use of a mathematical computer program either numerically or in a symbolic form.

From  $A_{S0}(t)$ , the asymptotic and steady-state availability  $A_{S0}(\infty) = A_S$  follows immediately. Alternatively, setting  $P_{i(\infty)} = P_i$  ( $i = 0, 1, 2$ ) for the asymptotic and steady-state value of the state probabilities,  $A_S$  follows as  $A_S = P_0 + P_1$  with  $P_i$  as solution of the following equations (see Annex A)

$$\begin{aligned} 0 &= -2\lambda P_0 + \mu P_1 \\ 0 &= 2\lambda P_0 - (\lambda + \mu)P_1 + 2\mu P_2 \\ 0 &= \lambda P_1 - 2\mu P_2 \end{aligned}$$

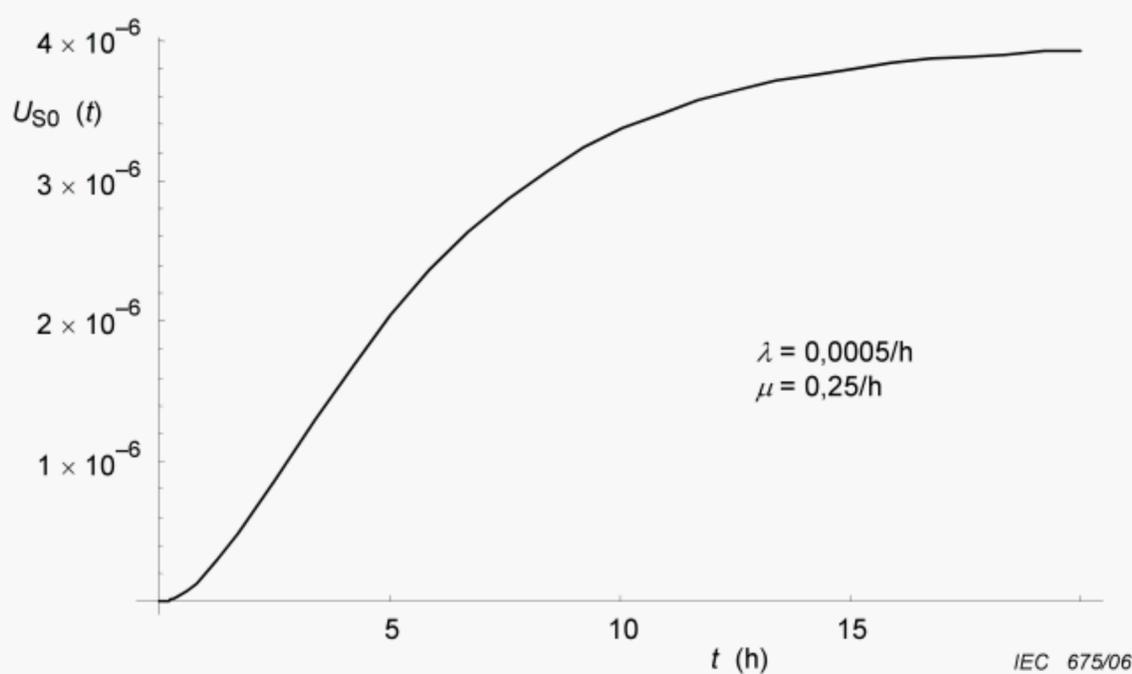
In the above set of algebraic equations, any one can be obtained from the other two, so that there are really only two useful equations and three unknowns. To overcome this difficulty, the fact that  $P_0 + P_1 + P_2 = 1$  is used as the third equation. Hence, after some mathematical manipulation, it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

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

The indices  $S0$  in  $A_{S0}(t)$  make clear that one deals with the availability at system level for the system starting in state 0 at  $t=0$ . For this simple model, an explicit expression in  $\lambda$  and  $\mu$  can be calculated by e. g. using Laplace transforms and is given by

$$A_{S0}(t) = \frac{\mu^2 + 2\lambda\mu}{(\lambda + \mu)^2} + \left( \frac{\lambda}{\lambda + \mu} \right)^2 e^{-(\lambda+\mu)t} (2 - e^{-(\lambda+\mu)t})$$

Figure C.3 shows a numerical example for the unavailability  $U_{S0}(t) = 1 - A_{S0}(t)$ .



**Figure C.3 – Numerical example for unavailability**

In the general case, the differential equations would have to be evaluated by use of a mathematical computer program either numerically or in a symbolic form.

From  $A_{S0}(t)$ , the asymptotic and steady-state availability  $A_{S0}(\infty) = A_S$  follows immediately. Alternatively, setting  $P_{i(\infty)} = P_i$  ( $i = 0, 1, 2$ ) for the asymptotic and steady-state value of the state probabilities,  $A_S$  follows as  $A_S = P_0 + P_1$  with  $P_i$  as solution of the following equations (see Annex A)

$$\begin{aligned} 0 &= -2\lambda P_0 + \mu P_1 \\ 0 &= 2\lambda P_0 - (\lambda + \mu)P_1 + 2\mu P_2 \\ 0 &= \lambda P_1 - 2\mu P_2 \end{aligned}$$

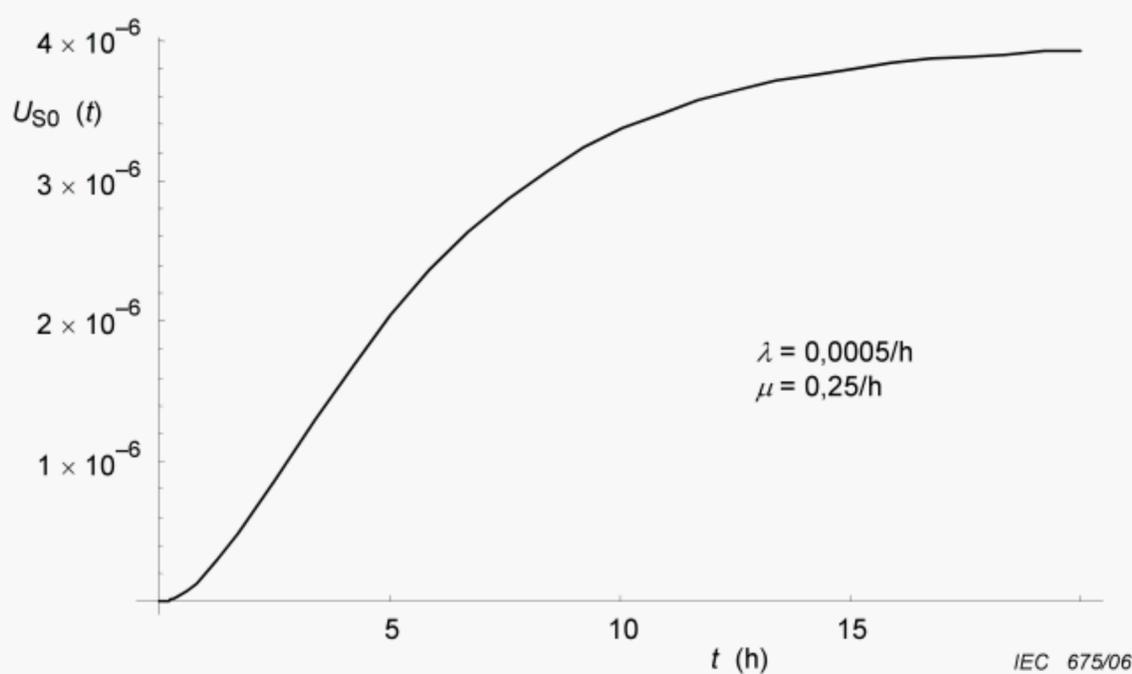
In the above set of algebraic equations, any one can be obtained from the other two, so that there are really only two useful equations and three unknowns. To overcome this difficulty, the fact that  $P_0 + P_1 + P_2 = 1$  is used as the third equation. Hence, after some mathematical manipulation, it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

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

The indices  $S0$  in  $A_{S0}(t)$  make clear that one deals with the availability at system level for the system starting in state 0 at  $t=0$ . For this simple model, an explicit expression in  $\lambda$  and  $\mu$  can be calculated by e. g. using Laplace transforms and is given by

$$A_{S0}(t) = \frac{\mu^2 + 2\lambda\mu}{(\lambda + \mu)^2} + \left(\frac{\lambda}{\lambda + \mu}\right)^2 e^{-(\lambda+\mu)t} (2 - e^{-(\lambda+\mu)t})$$

Figure C.3 shows a numerical example for the unavailability  $U_{S0}(t) = 1 - A_{S0}(t)$ .



**Figure C.3 – Numerical example for unavailability**

In the general case, the differential equations would have to be evaluated by use of a mathematical computer program either numerically or in a symbolic form.

From  $A_{S0}(t)$ , the asymptotic and steady-state availability  $A_{S0}(\infty) = A_S$  follows immediately. Alternatively, setting  $P_{i(\infty)} = P_i$  ( $i = 0, 1, 2$ ) for the asymptotic and steady-state value of the state probabilities,  $A_S$  follows as  $A_S = P_0 + P_1$  with  $P_i$  as solution of the following equations (see Annex A)

$$\begin{aligned} 0 &= -2\lambda P_0 + \mu P_1 \\ 0 &= 2\lambda P_0 - (\lambda + \mu)P_1 + 2\mu P_2 \\ 0 &= \lambda P_1 - 2\mu P_2 \end{aligned}$$

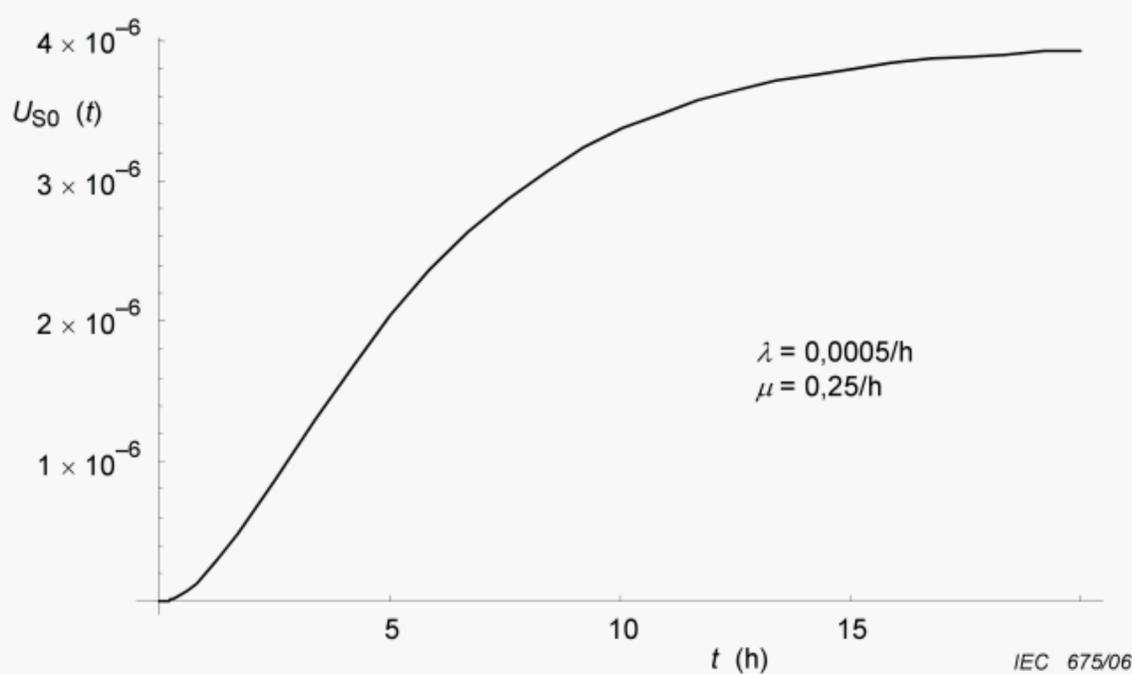
In the above set of algebraic equations, any one can be obtained from the other two, so that there are really only two useful equations and three unknowns. To overcome this difficulty, the fact that  $P_0 + P_1 + P_2 = 1$  is used as the third equation. Hence, after some mathematical manipulation, it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

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

The indices  $S0$  in  $A_{S0}(t)$  make clear that one deals with the availability at system level for the system starting in state 0 at  $t=0$ . For this simple model, an explicit expression in  $\lambda$  and  $\mu$  can be calculated by e. g. using Laplace transforms and is given by

$$A_{S0}(t) = \frac{\mu^2 + 2\lambda\mu}{(\lambda + \mu)^2} + \left(\frac{\lambda}{\lambda + \mu}\right)^2 e^{-(\lambda+\mu)t} (2 - e^{-(\lambda+\mu)t})$$

Figure C.3 shows a numerical example for the unavailability  $U_{S0}(t) = 1 - A_{S0}(t)$ .



**Figure C.3 – Numerical example for unavailability**

In the general case, the differential equations would have to be evaluated by use of a mathematical computer program either numerically or in a symbolic form.

From  $A_{S0}(t)$ , the asymptotic and steady-state availability  $A_{S0}(\infty) = A_S$  follows immediately. Alternatively, setting  $P_{i(\infty)} = P_i$  ( $i = 0, 1, 2$ ) for the asymptotic and steady-state value of the state probabilities,  $A_S$  follows as  $A_S = P_0 + P_1$  with  $P_i$  as solution of the following equations (see Annex A)

$$\begin{aligned} 0 &= -2\lambda P_0 + \mu P_1 \\ 0 &= 2\lambda P_0 - (\lambda + \mu)P_1 + 2\mu P_2 \\ 0 &= \lambda P_1 - 2\mu P_2 \end{aligned}$$

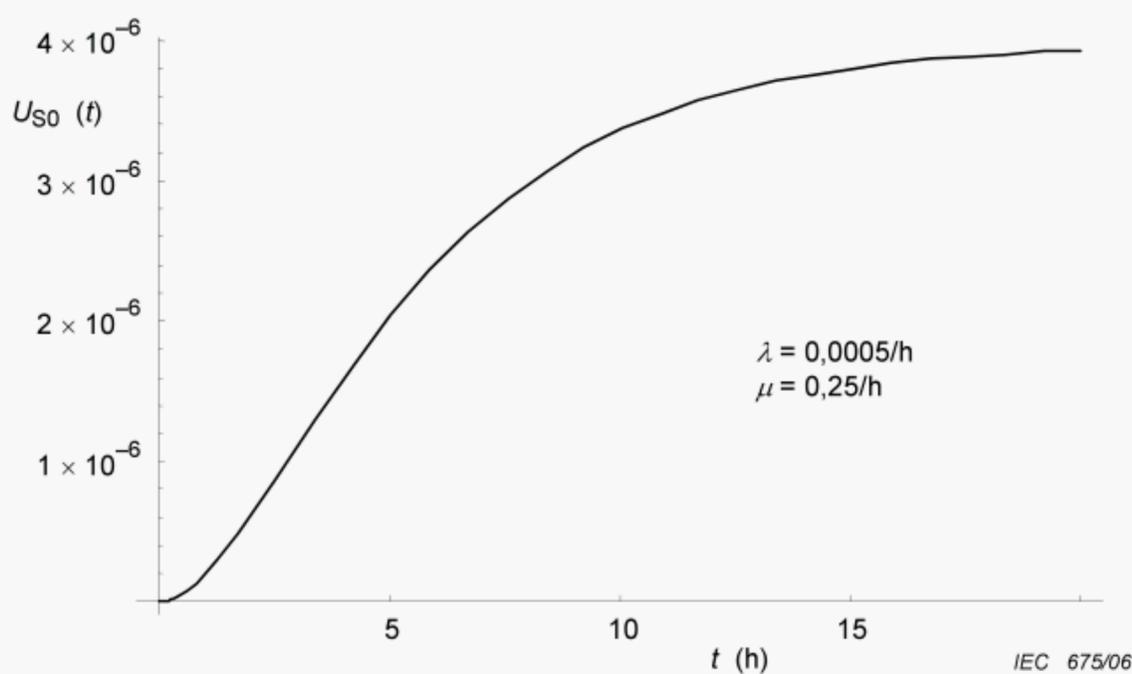
In the above set of algebraic equations, any one can be obtained from the other two, so that there are really only two useful equations and three unknowns. To overcome this difficulty, the fact that  $P_0 + P_1 + P_2 = 1$  is used as the third equation. Hence, after some mathematical manipulation, it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

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

The indices  $S0$  in  $A_{S0}(t)$  make clear that one deals with the availability at system level for the system starting in state 0 at  $t=0$ . For this simple model, an explicit expression in  $\lambda$  and  $\mu$  can be calculated by e. g. using Laplace transforms and is given by

$$A_{S0}(t) = \frac{\mu^2 + 2\lambda\mu}{(\lambda + \mu)^2} + \left(\frac{\lambda}{\lambda + \mu}\right)^2 e^{-(\lambda+\mu)t} (2 - e^{-(\lambda+\mu)t})$$

Figure C.3 shows a numerical example for the unavailability  $U_{S0}(t) = 1 - A_{S0}(t)$ .



**Figure C.3 – Numerical example for unavailability**

In the general case, the differential equations would have to be evaluated by use of a mathematical computer program either numerically or in a symbolic form.

From  $A_{S0}(t)$ , the asymptotic and steady-state availability  $A_{S0}(\infty) = A_S$  follows immediately. Alternatively, setting  $P_{i(\infty)} = P_i$  ( $i = 0, 1, 2$ ) for the asymptotic and steady-state value of the state probabilities,  $A_S$  follows as  $A_S = P_0 + P_1$  with  $P_i$  as solution of the following equations (see Annex A)

$$\begin{aligned} 0 &= -2\lambda P_0 + \mu P_1 \\ 0 &= 2\lambda P_0 - (\lambda + \mu)P_1 + 2\mu P_2 \\ 0 &= \lambda P_1 - 2\mu P_2 \end{aligned}$$

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

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