

BS EN 62551:2012



BSI Standards Publication

Analysis techniques for dependability — Petri net techniques

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

raising standards worldwide™



National foreword

This British Standard is the UK implementation of EN 62551:2012. It is identical to IEC 62551:2012.

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

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

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

© The British Standards Institution 2012.

Published by BSI Standards Limited 2012

ISBN 978 0 580 61353 1

ICS 21.020

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2012.

Amendments issued since publication

Date	Text affected
-------------	----------------------

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 62551

November 2012

ICS 21.020

English version

**Analysis techniques for dependability -
Petri net techniques
(IEC 62551:2012)**

Techniques d'analyse de sûreté de
fonctionnement -
Techniques des réseaux de Petri
(CEI 62551:2012)

Analysemethoden für Zuverlässigkeit -
Petrinetze
(IEC 62551:2012)

This European Standard was approved by CENELEC on 2012-11-06. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

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

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

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

CENELEC

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

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Foreword

The text of document 56/1476/FDIS, future edition 1 of IEC 62551, prepared by IEC/TC 56 "Dependability" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62551:2012.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2013-08-06
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2015-11-06

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 62551:2012 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 61508 Series	NOTE	Harmonised as EN 61508 Series (not modified).
IEC 61508-4:2010	NOTE	Harmonised as EN 61508-4:2010 (not modified).
IEC 61508-1:2010	NOTE	Harmonised as EN 61508-1:2010 (not modified).
IEC 61165:2006	NOTE	Harmonised as EN 61165:2006 (not modified).
IEC 60812:2006	NOTE	Harmonised as EN 60812:2006 (not modified).
IEC 61025:2006	NOTE	Harmonised as EN 61025:2007 (not modified).
IEC 61078:2006	NOTE	Harmonised as EN 61078:2006 (not modified).
IEC 61511-3:2003	NOTE	Harmonised as EN 61511-3:2004 (not modified).
IEC 61703:2001	NOTE	Harmonised as EN 61703:2002 (not modified).

Annex ZA
(normative)

**Normative references to international publications
with their corresponding European publications**

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

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 60050-191	1990	International Electrotechnical Vocabulary (IEV) - Chapter 191: Dependability and quality of service	-	-

CONTENTS

INTRODUCTION.....	7
1 Scope.....	8
2 Normative references	8
3 Terms, definitions, symbols and abbreviations.....	8
3.1 Terms and definitions	8
3.2 Symbols and abbreviations.....	10
4 General description of Petri nets	12
4.1 Untimed low-level Petri nets	12
4.2 Timed low-level Petri nets	12
4.3 High-level Petri nets	13
4.4 Extensions of Petri nets and modelling with Petri nets	13
4.4.1 Further representations of Petri net elements	13
4.4.2 Relationship to the concepts of dependability	14
5 Petri net dependability modelling and analysis.....	15
5.1 The steps to be performed in general	15
5.2 Steps to be performed in detail.....	16
5.2.1 General	16
5.2.2 Description of main parts and functions of the system (Step 1)	16
5.2.3 Modelling the structure of the system on the basis of Petri net- submodels and their relations (Step 2).....	16
5.2.4 Refining the models of Step 2 until the required level of detail is achieved (Step 3)	18
5.2.5 Analysing the model to achieve the results of interest (Step 4)	18
5.2.6 Representation and interpretation of results of analyses (Step 5)	19
5.2.7 Summary of documentation (Step 6).....	20
6 Relationship to other dependability models.....	20
Annex A (informative) Structure and dynamics of Petri nets	22
Annex B (informative) Availability with redundancy m-out-of-n	33
Annex C (informative) Abstract example	39
Annex D (informative) Modelling typical dependability concepts.....	43
Annex E (informative) Level-crossing example.....	45
Bibliography.....	62
Figure 1 – Weighted inhibitor arc	13
Figure 2 – Place p is a multiple place.....	14
Figure 3 – Marking on p after firing of transition t	14
Figure 4 – The activation of t depends on the value of V	14
Figure 5 – Methodology consisting mainly of ‘modelling’, ‘analysing’ and ‘representing’ steps.....	15
Figure 6 – Process for dependability modelling and analysing with Petri nets	15
Figure 7 – Modelling structure concerning the two main parts ‘plant’ and ‘control’ with models for their functions and dependability	17
Figure 8 – Indication of the analysis method as a function of the PN model	19

Figure A.1 – Availability state-transition circle of a component	22
Figure A.2 – Transition ‘failure’ is enabled	23
Figure A.3 – ‘Faulty’ place marked due to firing of ‘failure’	23
Figure A.4 – Transition ‘comp ₁ repair’ is enabled.....	24
Figure A.5 – The token at the ‘maintenance crew available’ location is not used	24
Figure A.6 – Transition is not enabled.....	25
Figure A.7 – Marking before firing	25
Figure A.8 – Marking after firing	25
Figure A.9 – PN with initial marking	25
Figure A.10 – Corresponding RG	25
Figure A.11 – Transitions ‘comp _{1p} repair’ and ‘comp _{np} failure’ are enabled	26
Figure A.12 – Marking after firing of transition ‘comp _{1p} repair’	27
Figure A.13 – A timed PN with two exponentially distributed timed transitions.....	28
Figure A.14 – The corresponding stochastic reachability graph	28
Figure A.15 – Petri net with timed transitions	29
Figure B.1 – Two individual item availability nets with specific failure- and repair-rates.....	33
Figure B.2 – Stochastic reachability graph corresponding to Figure B.1 with global states (as an abbreviation \bar{c}_1 is used for “comp ₁ faulty”).....	33
Figure B.3 – Three individual item availability nets with specific failure rates and repair rates	33
Figure B.4 – Stochastic reachability graph corresponding to Figure B.3 with global states (as an abbreviation \bar{c}_1 is used for ‘comp ₁ faulty’)	34
Figure B.5 – Specifically connected 1-out-of-3 availability net	35
Figure B.6 – Specifically connected 2-out-of-3 availability net	35
Figure B.7 – Specifically connected 3-out-of-3 availability net	36
Figure B.8 – Stochastic reachability graph with system specific operating states	36
Figure B.9 – Specifically connected 1-out-of-3 reliability net	37
Figure B.10 – Reachability graph for the net in Figure B.9	37
Figure B.11 – Specifically connected 2-out-of-3 reliability net	37
Figure B.12 – Reachability graph for the net in Figure B.11	37
Figure B.13 – Specifically connected 3-out-of-3 reliability net	38
Figure B.14 – Reachability graph for the net in Figure B.13	38
Figure C.1 – Individual availability net.....	39
Figure C.2 – Stochastic availability graph of the net in Figure C.1 with its global states and aggregated global states according to availability and safety	39
Figure C.3 – Basic reliability and function modelling concept	40
Figure C.4 – General hierarchical net with supertransitions to model reliability	41
Figure C.5 – General hierarchical net with supertransitions and superplaces	41
Figure C.6 – General hierarchical net with supertransitions to model availability	41
Figure C.7 – General hierarchical net with supertransitions and superplaces	42
Figure E.1 – Applied example of a level crossing and its protection system	45
Figure E.2 – Main parts of the level crossing example model	46
Figure E.3 – Submodels of the level crossing example model	47
Figure E.4 – PN model of car and train traffic processes.....	48

Figure E.5 – PN model of the traffic processes and traffic dependability	49
Figure E.6 – PN model of the traffic process with an ideal control function.....	50
Figure E.7 – PN model of the level crossing example model	51
Figure E.8 – Collected measures of the road traffic flow of a particular level crossing: Time intervals between two cars coming to the level crossing	52
Figure E.9 – Approximated probability distribution function based on the measures depicted in Figure E.5	53
Figure E.10 – Collected measurements of time spent by road vehicle in the danger zone of the level crossing	53
Figure E.11 – Approximated probability distribution function based on measurements depicted in Figure E.10	54
Figure E.12 – Aggregated RG and information about the corresponding states	59
Figure E.13 – Results of the quantitative analysis showing the level crossing average availability for road traffic users as a function of the protection equipment hazard rate for different used activation and approaching times T_{AC}	60
Figure E.14 – Results of the quantitative analysis showing the individual risk of the level crossing users as a function of the protection equipment hazard rate for different used activation and approaching times T_{AC}	60
Figure E.15 – Availability safety diagram based on the quantitative results of the model analysis shown in Figure E.13 and Figure E.14	61
Table 1 – Symbols in untimed Petri nets	10
Table 2 – Additional symbols in timed Petri nets	11
Table 3 – Symbols for hierarchical modelling	11
Table 4 – Corresponding concepts in systems, Petri nets and dependability	15
Table 5 – Mandatory and recommended parts of documentation	20
Table A.1 – Corresponding concepts in systems, Petri nets, reachability graphs and dependability	26
Table A.2 – Place and transition with rewards.....	32
Table D.1 – Dependability concepts modelled with PN structures	43
Table D.2 – Modelling costs of states and events.....	44
Table E.1 – Car-related places in the submodel ‘Traffic process’ (see Figure E.4)	52
Table E.2 – Car-traffic related transitions in the submodel ‘Traffic process’ and Traffic dependability (see Figure E.7)	55
Table E.3 – Train-traffic related places in the submodel ‘Traffic process’ (see Figure E.7).....	55
Table E.4 – Train-traffic related transitions in the submodel ‘Traffic process’ (see Figure E.7).....	56
Table E.5 – Places in the submodel ‘Traffic dependability’ (see Figure E.7).....	56
Table E.6 – Transitions in the submodel ‘Traffic dependability’ (see Figure E.7)	56
Table E.7 – Places in the submodel ‘Control function’ (see Figure E.7).....	57
Table E.8 – Transitions in the submodel ‘Control function’ (see Figure E.7)	57
Table E.9 – Places in the submodel ‘Control equipment dependability’ (see Figure E.7)	57
Table E.10 – Transitions in the submodel ‘Control equipment dependability’ (see Figure E.7).....	58
Table E.11 – Specification of boolean conditions for states to be subsumed in an aggregated state.....	59

INTRODUCTION

This International Standard provides a basic methodology for the representation of the basic elements of Petri nets (PNs) [1]¹ and provides guidance for application of the techniques in the dependability field.

The inherent power of Petri net modelling is its ability to describe the behaviour of a system by modelling the relationship between local states and local events. Against this background, Petri nets have gained widespread acceptance in many industrial fields of application (e.g. information, communication, transportation, production, processing and manufacturing and power engineering).

The conventional methods are very limited when dealing with actual industrial systems because they are neither able to handle multi-state systems, nor able to model dynamic system behaviour (e.g. fault tree or reliability Block diagrams), and can be subject to the combinatorial explosion of the states to be handled (e.g. Markov process). Therefore, alternative modelling and calculating methods are needed.

Dependability calculations of an industrial system intend to model the various states of the system and how it evolves from one state to another when events (failures, repairs, periodic tests, night, day, etc.) occur.

Reliability engineers need a user-friendly graphical support to achieve their models. Due to their graphical presentation, Petri nets are a very promising modelling technique for dependability modelling and calculations.

Analytical calculations are limited to small systems and/or by strong hypothesis (e.g. exponential laws, low probabilities) to be fulfilled. A qualitative increase is needed to deal with industrial size systems. This may be done by going from analytical calculation to Monte Carlo simulation.

This standard aims at defining the consolidated basic principles of the PNs in the context of dependability and the current usage of Petri net PN modelling and analysing as a means for qualitatively and quantitatively assessing the dependability and risk-related measures of a system.

¹ Figures in square brackets refer to the bibliography.

ANALYSIS TECHNIQUES FOR DEPENDABILITY – PETRI NET TECHNIQUES

1 Scope

This International Standard provides guidance on a Petri net based methodology for dependability purposes. It supports modelling a system, analysing the model and presenting the analysis results. This methodology is oriented to dependability-related measures with all the related features, such as reliability, availability, production availability, maintainability and safety (e.g. safety integrity level (SIL) [2] related measures).

This standard deals with the following topics in relation to Petri nets:

- a) defining the essential terms and symbols and describing their usage and methods of graphical representation;
- b) outlining the terminology and its relation to dependability;
- c) presenting a step-by-step approach for
 - 1) dependability modelling with Petri nets,
 - 2) guiding the usage of Petri net based techniques for qualitative and quantitative dependability analyses,
 - 3) representing and interpreting the analysis results;
- d) outlining the relationship of Petri nets to other modelling techniques;
- e) providing practical examples.

This standard does not give guidance on how to solve mathematical problems that arise when analysing a PN; such guidance can be found in [3] and [4].

This standard is applicable to all industries where qualitative and quantitative dependability analyses is performed.

2 Normative references

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

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

3 Terms, definitions, symbols and abbreviations

For the purposes of this document, the terms and definitions given in IEC 60050-191, as well as the following terms and definitions, apply.

3.1 Terms and definitions

3.1.1

component

constituent part of a device which cannot be physically divided into smaller parts without losing its particular function

[SOURCE: IEC 60050-151:2001, 151-11-21] [5]

3.1.2 event

something that happens in time

Note 1 to entry: In pure physics, an event is considered as a point in space-time.

[SOURCE: IEC 60050-111, Amendment 1:2005, 111-16-04] [6]

3.1.3 system

set of interrelated elements considered in a defined context as a whole and separated from their environment

Note 1 to entry: A system is generally defined with the view of achieving a given objective, e.g. by performing a definite function.

Note 2 to entry: Elements of a system may be natural or man-made material objects, as well as modes of thinking and the results thereof (e.g. forms of organization, mathematical methods, programming languages).

Note 3 to entry: The system is considered to be separated from the environment and the other external systems by an imaginary surface, which cuts the links between them and the system.

Note 4 to entry: The term 'system' should be qualified when it is not clear from the context to what it refers, e.g. control system, colorimetric system, system of units, transmission system.

[SOURCE: IEC 60050-351:2006, 351-21-20] [7]

3.1.4 safety integrity level

SIL

discrete level (one out of a possible four) corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

Note 1 to entry: The target failure measures (see 3.5.17 of IEC 61508-4:2010) [8] for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1:2010 [9].

[SOURCE: IEC 61508-4:1998, 3.5.8, modified]

3.1.5 Petri net

PN

bipartite graph with two kinds of nodes, places and transition, and directed arcs, to model local states and local events, respectively

Note 1 to entry: Petri-net are often used to model the behaviour of distributed systems.

3.1.6 directed arc

oriented connection of a pair of nodes depicted by a line with arrow

Note 1 to entry: In general, the arcs in Petri nets are directed. They can only connect two different types of nodes.

Note 2 to entry: In addition to directed arcs. alternative representations exist.

3.1.7 place

type of node in a Petri-net to model local states or conditions

3.1.8 transition

type of node in a Petri-net to model local events, i.e. state changes

3.1.9 transition type

type of transition modelling a particular event of a group of events belonging to a given class

Note 1 to entry: In general, there exist various types of transitions in a Petri-net, e.g. to model causal events, to model events taking place after a certain time delay, etc.

3.1.10 supernode

type of node in a Petri-net to hide subnets, especially used in models with hierarchies

3.1.11 superarc

type of arc in a Petri-net that hides the various connections of two supernodes

Note 1 to entry: These two supernodes hide two subnets that may be connected with various kinds of arcs.

3.1.12 reachability graph

RG
state transition diagram, representing the behaviour of a system

Note 1 to entry: The reachability graph may be generated on the basis of a Petri-net with an initial marking.

3.1.13 marking




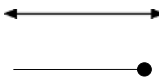
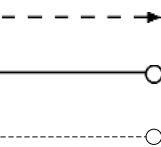

graphical representation of the state of the system that is modelled by a Petri-net

3.2 Symbols and abbreviations

NOTE The graphical representation of a Petri net requires symbols, identifiers and labels which should be used in a consistent manner. A collection of commonly used graphical representations is given in Table 1, Table 2 and Table 3.





The following symbols in Table 1 are recommended in untimed Petri nets. The label 'n' of the normal arc specifies an integer value.

Table 1 – Symbols in untimed Petri nets

<i>identifier</i> 	<i>identifier</i> 	<i>identifier</i>  (<i>weight</i>)	\xrightarrow{n} (normal) arc			
Place symbol, also used for multiple places	Transition symbol	Transition symbol with a transition weight	Relation symbols – normal arcs	Relation symbols – test arcs	Relation symbols – inhibitor arcs	Token symbol




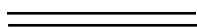
There are various possibilities to draw test- and inhibitor-arcs. The token symbol is not a symbol of the static structure of the net but is used to symbolize the flow of information.

Table 2 – Additional symbols in timed Petri nets

	Type of transition			
	Deterministic		Stochastic	
	Delay is zero	Delay is d	Exponentially or geometrically distributed	Arbitrarily distributed
Parameter		d	λ	\emptyset Arbitrary distribution
Symbol				

NOTE In case of deterministic transitions, a Dirac distribution is often used. Furthermore, the parameters of timed transition may be state- or time-dependent.

Table 3 – Symbols for hierarchical modelling

<i>Identifier</i> 	<i>Identifier</i> 	<i>Identifier</i> 	
Superplace symbol	Supertransition symbol	Supernode symbol	Superarc symbol
Note that the symbol of a 'superarc' does not have a direction, because it may substitute more than one arc with different directions.			

Abbreviation	Meaning
CDF	Cumulative distribution function
ETA	Event tree analysis
DZ	Danger zone
FME(C)A	Failure, mode, effects (and criticality) analysis
FTA	Fault tree analysis
HR	Hazard rate
LC	Level crossing
MTBF	Mean time between failures
MTTF	Mean time to failure
PN	Petri net
RBD	Reliability block diagram
RG	Reachability graph
SIL	Safety integrity level
ir	Impulse reward
rr	Rate reward

4 General description of Petri nets

4.1 Untimed low-level Petri nets

Petri nets (PNs) are graphs in which active and passive nodes are differentiated. The passive elements are called places; they model local states or conditions for example, and are marked with tokens if the local state is fulfilled. The active elements are called transitions. They model the possible changes from one state to another (e.g. the potential events that may occur). Places and transitions may be called nodes. The causal relations between the phenomena represented by places and transitions are explicitly described through various kinds of directed arcs that connect these nodes (see the basic symbols of a Petri net in Table 1 and Clause A.1 for an introduction to PNs). Inhibitor arcs can only connect preset places with transitions in their postset (see A.1.2).

A transition is enabled, if all its preset places that are connected with it by normal arcs or test arcs are marked with a sufficient number of tokens and if all its preset places that are connected with it by inhibitor arcs are unmarked. The number of tokens that are sufficient for the enabling of a transition is annotated to the arc. In general, this annotation can be marking dependent (see [3]). See 4.4 for commonly used generalizations of these concepts.

If a transition is enabled, it may fire, i.e. it may change the marking of the model. The firing of a transition only changes the marking of places that are connected with it by normal arcs: firing leads to absorbing tokens from corresponding places in its preset and to the production of tokens in its postset. The number of tokens that is absorbed and produced is specified by the arc label. If no arc label is given, the number is one.

That means that the places, transitions and arcs form the static elements and relations of a system, whereas the tokens may be produced or may vanish according to the states of the modelled system.

The reachability graph of a PN consists of all the global markings that can be reached from an initial marking through an arbitrary sequence of transition firings. In this graph, a node represents an individual global marking and each arc represents the firing of a transition that transforms one global marking to another.

PNs may be non graphically represented by incidence matrices. If T is the set of transitions and P is the set of places, then the incidence matrix is of dimension $|P| \times |T|$. For every transition, the changing of the global marking due to firing is specified in a corresponding column.

4.2 Timed low-level Petri nets

In timed PN, both untimed as well as timed transitions may be used. In order to fire, a timed transition shall be enabled for a specific time duration. This duration may be deterministic or stochastic, depending on the transition-specific distribution function (cumulative distribution function – CDF) and the corresponding parameters. If two or more transitions are enabled at the same time, then the firing of transitions is determined by a further specification of the transition, i.e. the ‘preselection policy’ or the ‘race policy’. In addition, choices about execution policy and memory policy, aside from the firing time distributions, shall be specified ([3]). After this duration has elapsed, the transition is allowed to fire. Table 2 shows the commonly used transitions in timed PNs.

Corresponding to the specific type of a timed transition, it may be attributed by a time parameter that specifies the fixed firing duration (transitions with deterministic firing time), the constant firing rate (transitions with exponential or geometric distributed firing times) or the probability distribution with its parameters (transitions with arbitrary distributed firing times). Note that untimed transitions are a particular case of fixed firing duration transitions with a deterministic delay of zero.

As in the untimed case, the RG of a timed PN consists of nodes representing global markings and of arrows, representing the firing of transitions. In addition to the untimed RG, the RG of a timed net shall take the specific parameters of the transitions into account.

4.3 High-level Petri nets

In high-level Petri nets, a marking consists of individual, distinguishable tuples instead of anonymous, black tokens. Thus, the tuples not only model the fulfillment of conditions or the existence of states, but also the information itself. Against this background, the arc labels can be formulated as a function of the existing information. Such a modelling support leads to compact and intuitive models, even for complex systems. As the methodology presented in this standard does not depend on these possibilities, for high-level PNs see ISO/IEC 15909-1 [10].

4.4 Extensions of Petri nets and modelling with Petri nets

NOTE When modelling with PNs, some commonly used notations, extensions and denotations are introduced in this subclause.

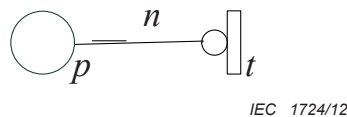
4.4.1 Further representations of Petri net elements

4.4.1.1 General

In addition to the symbols that have been introduced in Table 1 the following symbols and concepts for weighted inhibitor arcs, multiple places and global variables are also commonly used.

4.4.1.2 Weighted inhibitor arcs

As for normal arcs, inhibitor arcs can be weighted, see Figure 1.



IEC 1724/12

Figure 1 – Weighted inhibitor arc

Transition t in Figure 1 is enabled, only if the number of tokens on place p is lower than n . Note, that the marking shall actually be lower, if there are n tokens on place p , transition t is not enabled.

To improve the readability of complex nets, especially when modelling industrial sized systems, various additional concepts are commonly used.

4.4.1.3 Multiple places

If the same place appears multiple times in a net, these places are called ‘multiple places’, ‘repeated places’ or ‘fusion places’. In doing so, the modular structure of a model can be revealed. As multiple places are just identical copies of each other, their marking is the same in every marking of the net.

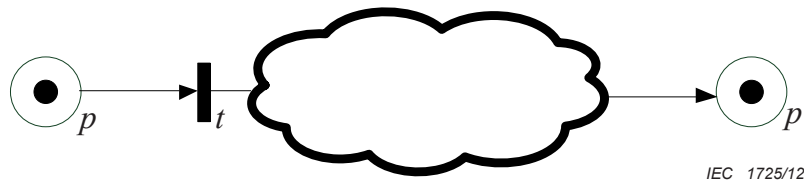


Figure 2 – Place p is a multiple place

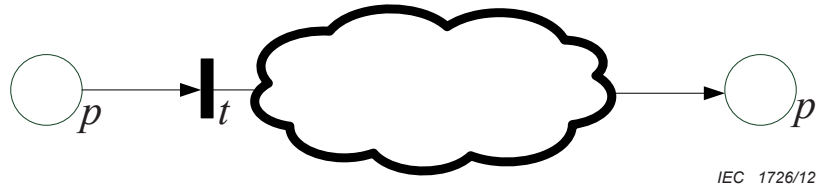


Figure 3 – Marking on p after firing of transition t

4.4.1.4 Global variables

The use of global variables is similar to that of multiple places. The activation of a transition can be conditioned on the value of global variables or predicates. In addition, firing such a transition may change the value of global variables through the use of assertions and predicates.

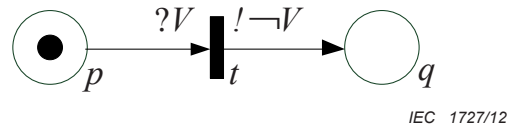


Figure 4 – The activation of t depends on the value of V

In the net in Figure 4, transition t in the depicted state is only enabled, if the global variable V is true ($?$ is a ‘reading’ operator, i.e. $?V$ serves as guard, reading the value of the global variable V). Firing t will mark place q , unmark place p and set V to false ($!$ is a ‘writing’ operator, i.e. $!¬V$ sets the value of the global variable V to false: $¬V$ means ‘not V ’). In this context, one often speaks of ‘read’ and ‘write’ actions or of assertions.

4.4.2 Relationship to the concepts of dependability

Petri nets of industrial size are often modularized in various communicating sub-Petri nets, see e.g. [11] and [12].

In the context of dependability, local events, such as failures or repairs, can be modelled by transitions, and local states, such as faults, can be modelled by places. Therefore, the name associated with every node primarily represents the corresponding dependability feature and indicates the related device, if required. If the concepts of PNs are interpreted in this way, one can speak of ‘dependability interpreted PNs’.

Table 4 gives an overview of corresponding concepts between systems in general, Petri nets and concepts of dependability. It does not include all possible interpretations of failures or faulty states.

Table 4 – Corresponding concepts in systems, Petri nets and dependability

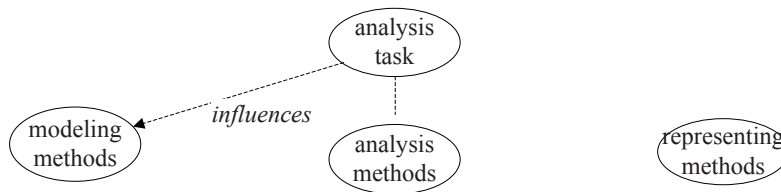
Aspect	System	Petri net	Dependability	
Dynamic	Event	Transition	Failure	Repair
Static	Local state	Place	Faulty	Operating

NOTE Failure and repair are only examples of events relating to dependability; faulty and operating are only examples of states relating to dependability, further examples are first failure or degraded failures and states. These concepts may be used as a basis to calculate e.g. the average production availability.

5 Petri net dependability modelling and analysis

5.1 The steps to be performed in general

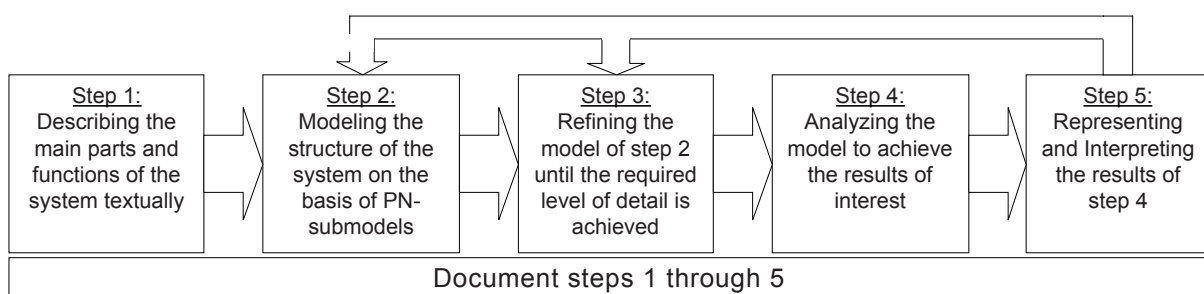
The analysis of a system requires in general an adequately detailed model of that system. The required level of detail depends on the analyses that are to be performed. Generally systems are too complex to be modelled on a detailed level in their entirety in only one step. Therefore, modelling shall be performed iteratively, starting with a rough textual description and ending in a detailed, formal model. The analysis results that are gained on the basis of the model shall be represented in a user-friendly way, and shall be interpreted against the background of the analysis task (see Figure 5).



IEC 1728/12

Figure 5 – Methodology consisting mainly of ‘modelling’, ‘analysing’ and ‘representing’ steps

Figure 6 depicts the main steps in dependability modelling and analysing with PNs. Although seemingly a straightforward process, the analyst has to bear in mind, that modelling in general is very much an iterative process. Step 3 in particular, ‘Refining the model’, will need several iterations.



IEC 1729/12

Figure 6 – Process for dependability modelling and analysing with Petri nets

Step 1: Describing the main parts of the system by conventional means of description, e.g. textually, with tables and figures etc. (see 5.2.2).

Step 2: Modelling the structure of the system on the basis of PN submodels and their relations, and documenting that model (see 5.2.3).

A system often consists of two main subsystems:

- a) the plant, i.e. the operational subsystem which has to be controlled;
- b) the control, i.e. the subsystem which serves to control the plant.

Step 3: Refining the model of Step 2 until the required level of detail is achieved and documenting that refined model (see 5.2.4).

A PN notation of the system of Step 2 including the subsystems shall be provided.

The required level of detail is reached when all the information that is necessary for the analyses is included in the model.

Step 4: Analysing the model to achieve the results of interest and documenting the analyses (see 5.2.5).

Step 5: Representing and interpreting the results of the analyses and documenting that representation (see 5.2.6).

If the results are not of adequate or required quality further (sub-) models may have to be added (return to Step 2) or existing (sub-) models may have to be refined (return to Step 3).

All individual steps and their results shall be continuously documented.

5.2 Steps to be performed in detail

5.2.1 General

In this subclause, the steps are described in more detail. In each step, the work that has been performed in that step shall be documented.

5.2.2 Description of main parts and functions of the system (Step 1)

The following concepts of the system that is to be modelled and analysed shall be identified and described as follows:

- a) boundaries, context and environment, especially related to dependability and requirements;
- b) main parts (for example the plant and the control equipment);
- c) main functions (operation and control/protection) and purpose.

This description can be done using free text, tables or figures as appropriate.

5.2.3 Modelling the structure of the system on the basis of Petri net-submodels and their relations (Step 2)

Dynamic systems, e.g. automation systems, can in general be divided into the subsystems 'uncontrolled plant' and 'control of the plant'. In order to prevent the plant from getting into undesired states, it is controlled by the control of the plant. In that way, the 'uncontrolled plant' becomes the 'controlled plant'. In addition, each of these subsystems can be interpreted from the functional and the dependability point of view. For example, as the control of the plant does not always work properly, one has to take the dependability of the control into account – the dependability of the system depends on the dependability of its control. As the model that is to be developed depends on the complexity of the system and on the analysis

task, the global model consists in general of a subset of the following four submodels (e.g. it may be the case that adequate results can be obtained without modelling the dependability of the plant), i.e. a submodel to specify:

- a) the functions of the plant;
- b) the dependability of the plant;
- c) the functions of the control;
- d) the dependability of the control.

In a) the operational subsystem that has to be controlled, i.e. the plant, shall be modelled. Without any control this dynamic subsystem would create a variety of processes within a huge state space, modelled by the RG of its PN. Some of the states in this RG have to be avoided because they represent hazards and lead to safety critical situations such as deadlocks, standstills, or other unavailable states.

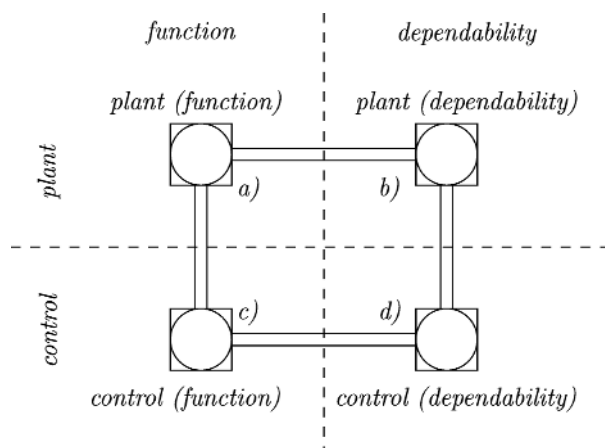
In b) the dependability of the plant shall be modelled. In this submodel, uncertainties concerning the behaviour of the plant shall be taken into account (e.g. human behaviour and environmental influences).

As the plant's dependability influences the availability, correctness, safety and other functions, the two submodels a) and b) are interconnected.

In c) the subsystem that serves to control the plant in order to restrict the operational process shall be specified. In this submodel, the possibility of failures of the control is not taken into account, one presumes that the control task is performed perfectly. In doing so, the appropriate connections with the models of a) and b) lead to a RG without any undesired (for example hazardous or accidental) states.

In d) the submodel that specifies the physical realization of the control with special respect to dependability is modelled. This model depends on the technical implementation or human operators and environmental influences. Through an adequate connection with the submodel of c), possible failures and improper behaviours of the control are considered. As these affect the control functions modelled in c), in the global model, i.e. the model that consists of the (connected) submodels of a) to d), the plant as well as the control and the control's dependability is considered. In this way, the corresponding RG contains hazardous and accidental states with their corresponding probabilities.

Regarding the different functional layers and their dependability aspects, the resulting orthogonal substructure is shown in Figure 7.



IEC 1730/12

Figure 7 – Modelling structure concerning the two main parts 'plant' and 'control' with models for their functions and dependability

An integrated model of the entire system can easily be established if each of the different subsystems is modelled by a single Petri net according to the previous subclauses. The single Petri net models are preferably connected by test and inhibitor arcs. This allows a modular approach. Hence any subsystem can be modified or changed individually without any side effects on its neighbouring models.

In the documentation of this step, the main submodels of the system that have been taken into account and their relations shall be identified. Here, the boundary of each submodel, their main parts, functions and purpose shall be documented by conventional means of description, e.g. textually, with tables or figures.

If it is not necessary (e.g. for very easy systems) or very difficult to split a system into these subsystems, the designer of the model shall state the reasons clearly and comprehensible.

5.2.4 Refining the models of Step 2 until the required level of detail is achieved (Step 3)

In this step, the model that has been developed in Step 2 shall be refined and the developed models shall be documented. This shall be done iteratively.

In this step, a PN model of the model performed in Step 2 shall be refined. This includes each of the subsystems that was taken into account.

This refinement shall be continued until the required level of detail has been reached, i.e. until all the information that is necessary for the analyses to be performed in Step 4 (see 5.2.5) is incorporated:

- a) It is mandatory that each node shall be labelled with a unique identifier. If one deals with timed nets, the time concept shall be clarified symbolically. It is recommended to use the symbols defined in 3.2.
- b) It is mandatory to specify the further details of the time concept, i.e. the specific parameters (e.g. weights of causal transitions, fixed durations, deterministic transitions, CDF with corresponding parameters of the stochastic transitions, etc.) as well as any transition guards, the memory policy of the transitions (are the activation times of a transition cumulated or is the transition memoryless? i.e. the preemption policy, see [3]), the place capacity, etc. This information can be included directly in the net if the readability is not affected. Otherwise, a representation by tables or matrices can be chosen.

The documentation of this step can be done by step-wise refinements according to the model refinement procedure. The documentation of this step shall contain:

- c) A PN representation of the subsystems and, if appropriate, of the whole model.
- d) A textual description of each of the subsystems (at least for the lowest modelled level).
- e) The basis for reliability parameters (e.g. failure and restoration, assumptions or statistical data) and for the system structure.

5.2.5 Analysing the model to achieve the results of interest (Step 4)

Concerning the tools, some commonly known PN-Tools can be found under [13].

The approach to be chosen to analyse the model by its nature depends on the results that are of interest. In addition, the applicable analysing methods (see Figure 8) are restricted by the underlying PN, and the availability of information. Basically, there are two alternatives:

- a) Qualitative analyses answer questions concerning the possibility of, for example, reaching a (global) state or of firing a certain transition sequence again and again.

Qualitative analyses are primarily based on the untimed RG. An untimed RG can be generated, at least theoretically, if, starting from the initial marking, only a finite number of

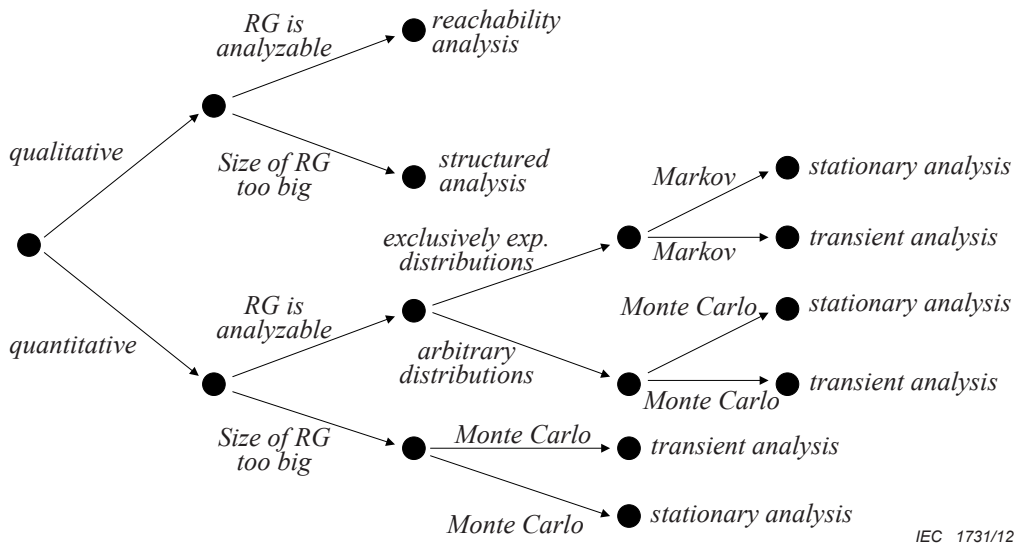
markings can be reached. Under specific conditions it is possible to derive from the untimed RG properties concerning the dynamic for the timed case ([14]). If the number of reachable markings is too great or even infinite, then alternative approaches exist: structural analyses, i.e. invariants, deadlocks and traps at least allow conclusions about quality measures for the modelled system ([11] and [14]).

- b) Quantitative analyses answer questions concerning the probability of qualitative results, e.g. the probability of reaching a certain state or the probability of firing a certain transition, reliability or dependability measures, such as failure probability, failure rate, MTTF or MTBF. These concepts may be used as a basis to calculate, for example, an average production availability.

Quantitative analyses are based primarily on the timed or stochastic RG. Like the untimed RG, one can analyse the timed RG if the number of reachable markings is not too great. Depending on the transitions that are in the PN, there are two alternatives:

- i) if all the transitions in the timed PN have an exponentially distributed firing duration over a defined period of time interest (i.e. they have a constant firing rate over a defined time period), one can transform the timed RG to a Markov chain and perform a stationary or transient analysis;
- ii) otherwise, the Monte Carlo simulation approach shall be used and a stationary or transient analysis performed.

If the number of reachable markings is too large, the Monte Carlo approach shall be used and transient analyses performed. The number of states that are manageable depends on soft- and hardware properties. Nowadays systems with about 10^8 states are still manageable. Systems with several million states may correspond to 'small' systems.



IEC 1731/12

Figure 8 – Indication of the analysis method as a function of the PN model

The documentation of this step shall contain:

- c) the methods chosen to calculate the results of interest must be listed;
- d) the tools that have been applied to do the calculations, the computing equipment and data conditions and default adjustments shall be listed.

5.2.6 Representation and interpretation of results of analyses (Step 5)

The output of this step shall fulfil the following requirements:

- a) the RG shall be represented adequately. In general, the concept of aggregated states will be necessary as the RG is too big if every single state is listed;

- b) the influence of different parameter values or system structures shall be represented adequately, e.g. the influence of different maintainability and reliability parameters as well as different system structures (e.g. redundancy schemes) on the availability and safety can be represented in an diagram that depicts the availability of the system as a function of its safety.

The results of the analysis shall be interpreted textually in a clear and concrete way. In addition, the analysis results should indicate alternative realizations (with respect to the system's structure or the implementation of the submodels).

5.2.7 Summary of documentation (Step 6)

Generally, the documentation corresponds to the requirements of quality management. In some areas, in particular safety critical applications, a specific documentation is mandatory, e.g. in railway, aviation, or in nuclear power plants, see Table 5.

Table 5 – Mandatory and recommended parts of documentation

No	Step	Representation of methods and means		
		Mandatory	Highly recommended	Recommended
1	General documentation: general description of the system, functions, parts and boundaries; objective and scope of the analysis; justification, why Petri net techniques are used	Text and figures Text Text		
2	Documentation of four submodels (see 5.2.3)	Text and figures	PN on a high-level	
3	Detailed documentation: system refinement models (abstraction layers); sources of data used (assumptions or statistical data?) for failure and restoration rates	Text and figures Text	Tables	b) Tables
4	Analysis methods: description of methods; description of computer and used tools	Text Text		a) Tables b) Tables
5	Results: in numerical and graphical form; interpretation of results	Text and figures Text		a) Tables

6 Relationship to other dependability models

Sometimes, only the cause-consequence chain of any item event, e.g. failure in the system, is of interest or vice versa the reasons for a system fault, i.e. a global state by means of a basic event or state, are of interest. These analyses result from FTA, ETA, RBD, or FMEA analysis techniques. The reachability graph includes all this information. Hence, these cause-effect relationships can be derived from the RG and represented in its traditional way ([10]).

This follows from the fact that the modelling power of PNs is higher than that of FTA, ETA and RBD. Thus, it can be shown that such models can be transformed into Petri nets without loss of information [15]. As Markov chains presume constant transition rates that imply exclusively exponentially distributed state durations, general stochastic PNs are of higher modelling

power. The information that is gained through performing a FMEA or FME(C)A, can be used to build the PN model of the system. Although FME(C)A in particular may provide a formal process with specified procedures and forms, they are not formal in a mathematical sense. In addition, they only allow analysis of single failures and should therefore not provide 'models' of the overall systems (except for the very simple case of serial systems). But as a basis to gather information about the system they may be very effective when they are used complementarily to PNs.

Annex A (informative)

Structure and dynamics of Petri nets

A.1 General Petri net concept and its relationship to reliability

A.1.1 Introductory remark

The overall view on Petri nets can be characterized and dependability interpreted as follows: active and passive elements are differentiated (see Table 1). The passive elements are called ‘places’; they model conditions, e.g. distinguishable elementary states with a certain duration. Transitions represent the active elements (e.g. events or logical rules) which change the elementary states on the basis of the firing rule.

Transitions are ‘activated’ when the necessary conditions are fulfilled, i.e. when the corresponding places carry a sufficient number of tokens. By switching a transition, i.e. the event, new conditions may become valid and the preconditions may lose their validity.

A.1.2 Petri net structure

As Petri nets are ‘bipartite’ graphs, each arc is connected with two different kinds of nodes. This means that between any two subsequent states (e.g. faulty and operating) there has to be an event that leads from one state to the other (e.g. repair). In addition, between any two subsequent events (e.g. failure and repair) there exists an intermediate state (e.g. faulty) – see Figure A.1 (here and in the following figures ‘comp₁ faulty’ is an abbreviation for ‘component₁ faulty and under repair’). Relations between states and events are represented by directed arcs. The ‘preset’ of a node n is the set of all nodes n_1 with a directed arc from n_1 to n . The ‘postset’ of n is the set of all nodes n_2 with a directed arc from n to n_2 . Beside ‘preset’ and ‘postset’, one often refers to these sets as ‘upstream’ and ‘downstream’ places.

PNs should model all relevant states which may hold and all possible cause-consequence relations which may occur, depending on conditions, i.e. a set of states.

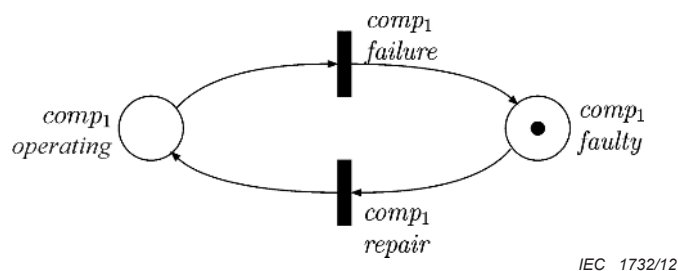


Figure A.1 – Availability state-transition circle of a component

A.1.3 Causal dynamics in low-level Petri nets

A.1.3.1 General

In PNs the dynamics of systems can be exemplified by visualizing the states and the system’s transitions of states with respect to their relations.

A.1.3.2 Marking

Places can be marked with tokens (‘black dots’) which depict the actual occurrence of a local state or ‘local marking’. The set of all local markings is called the ‘net’s marking’ or the ‘global

marking'. The net's marking before the firing of any of its transitions is called the 'initial marking'.

The marking of places can be changed by the 'switching' or 'firing' of transitions. This leads to the dynamics of nets that can be illustrated by the 'token flow':

A.1.3.3 Token flow and firing rule

A transition is enabled (i.e. it may 'fire') if all the places in its preset are marked with an appropriate number of tokens. A firing transition can remove tokens from preset places (corresponding to the types and the weights of the arcs connecting its preset places) and produces tokens on its postset places (see Figure A.2 and Figure A.3). That means that tokens are actually absorbed (or destructed) and produced, only simulating the nets behaviour makes them look like a flow. In general, the occurrence of a local event changes the local states in its direct neighbourhood. This can be interpreted as follows: if an event occurs (e.g. if a failure occurs) the state of the system is changed (here from 'operating' to 'faulty'). In addition, transitions can be weighted according to the probability of their occurrence: in a state with several enabled transitions, the transition with the highest weight will fire with the highest probability ([3]).

In relation to dependability, the occurrence of a failure changes the state of the system from 'operating' to 'faulty' and the condition 'overstressing' does not hold any more.

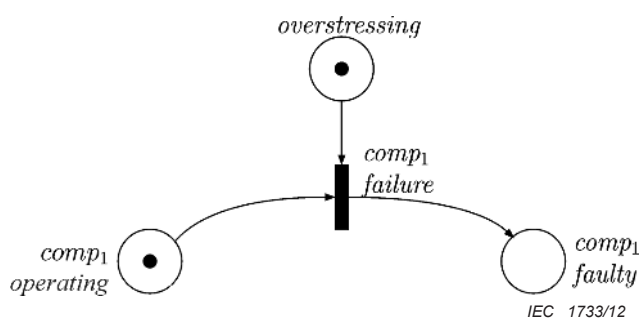


Figure A.2 – Transition 'failure' is enabled

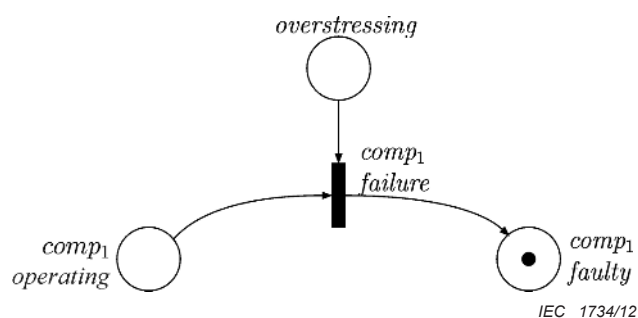
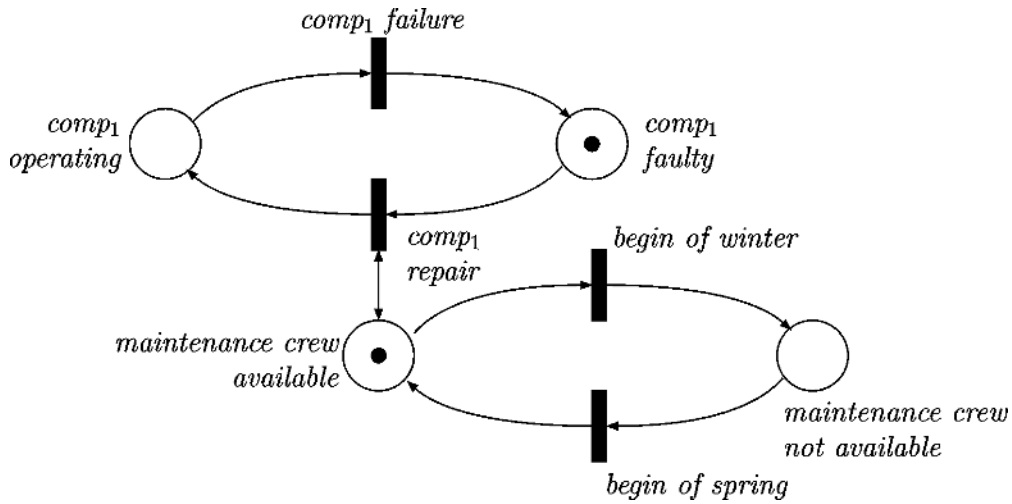


Figure A.3 – 'Faulty' place marked due to firing of 'failure'

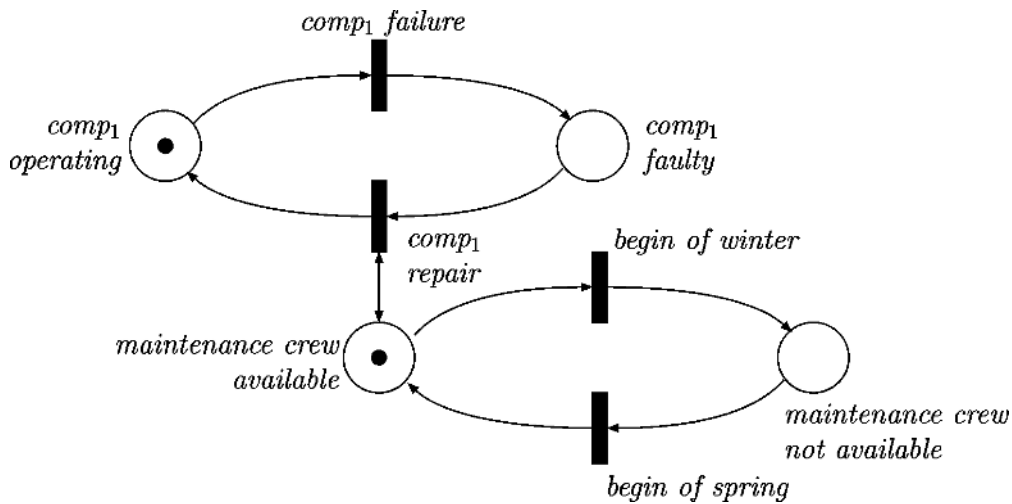
A.1.3.4 Test arcs

Transitions that are connected with a place via a 'test arc' or 'communication arc' do not change the number of tokens on that place. In this way, it is possible to read if a place is marked or not. Test arcs are drawn as double arrows (e.g. between 'maintenance crew' and 'repair' in Figures A.4 and A.5). Here, they prevent a repair occurring in winter (maintenance crew not available). It should be noted that this example is strongly simplified in order to concentrate on the meaning of test arcs.



IEC 1735/12

Figure A.4 – Transition ‘comp₁ repair’ is enabled



IEC 1736/12

Figure A.5 – The token at the ‘maintenance crew available’ location is not used

In Figure A.4 the transition ‘repair’ tests whether there is a ‘maintenance crew’ available, i.e. at least one token on this place. In this case the test succeeds. The transition is enabled and firing leads to the marking depicted in the net of Figure A.5.

A.1.3.5 Inhibitor arcs

Transitions that are connected via inhibitor arcs with their preset places are only enabled if the number of tokens of these places is strictly inferior to the weight of the corresponding inhibitor arcs, i.e. when the weights are equal to one, they are enabled only if the places do not carry any token. Inhibitor arcs are drawn with a small circle instead of an arrowhead. The firing of such a transition will not change the marking on the corresponding preset places.

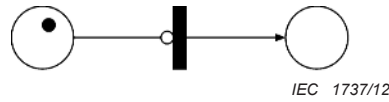


Figure A.6 – Transition is not enabled

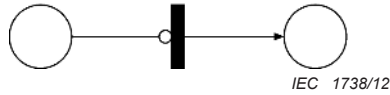


Figure A.7 – Marking before firing

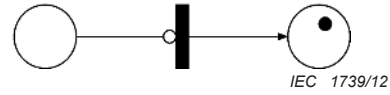


Figure A.8 – Marking after firing

As the transition in the nets in Figure A.6, Figure A.7 and Figure A.8 is only enabled if the place in its preset is unmarked, the transition in the net of Figure A.6 is not enabled. In the net of Figure A.7, the transition is enabled and firing leads to the marking depicted in the net of Figure A.8. It should be noted that in Figure A.8 the transition can be fired infinitely often; this can be prevented by a second inhibitor arc leading from the place in the postset of the transition to the transition. Just like ordinary arcs, inhibitor arcs can be weighted (see 4.4). An example of the application of an inhibitor arc can be found in A.1.3.

A.1.4 Reachability graph

The reachability graph (RG) of a PN represents all global markings that can be reached due to the firing of transitions, starting at a given 'initial marking'. Thus, the RG represents the possible behaviour of a system in explicitly depicting its state space.

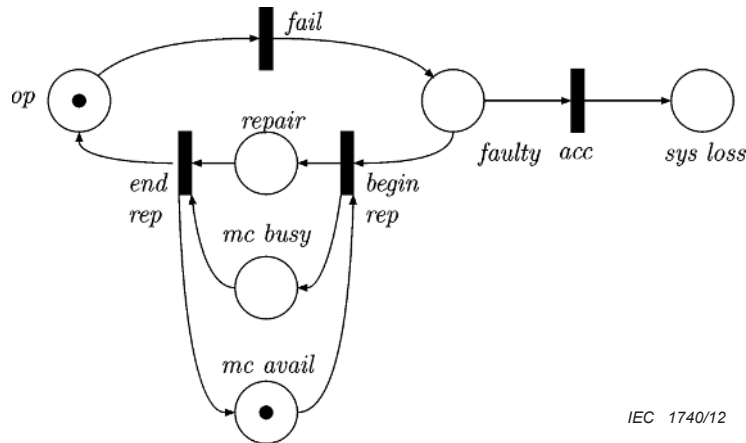


Figure A.9 – PN with initial marking

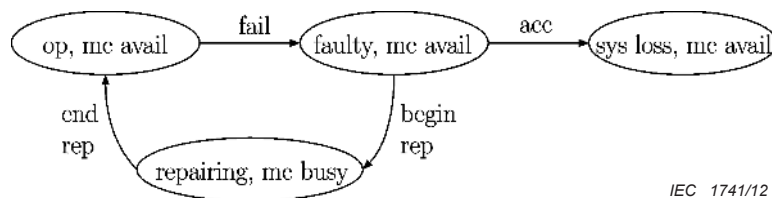


Figure A.10 – Corresponding RG

The space of reachable states of the Petri net in Figure A.9 consists of four global states (see Figure A.10). It should be noted that this example is strongly simplified in order to concentrate on the meaning of reachability graphs.

Each global state is drawn by a circle or ellipse which is definitely identified by the actual net marking. Due to its arc annotations, the RG specifies how the change from one global state to another is accomplished. For more complex Petri nets, the number of global states within the

RG may increase quickly with the number of components. The construction of its RG can be performed automatically by computer tools.

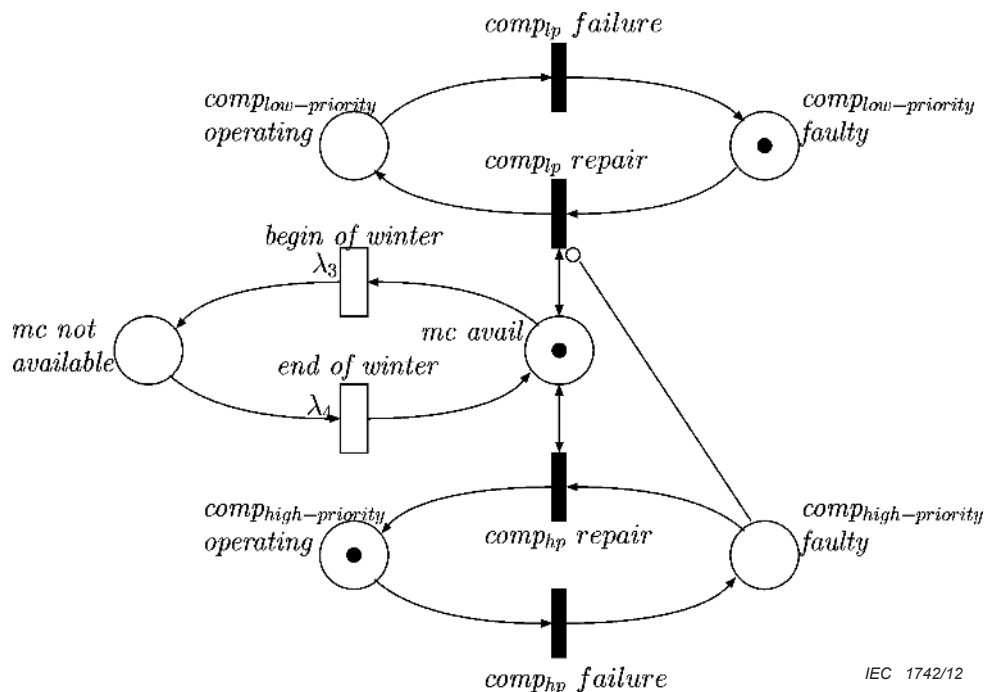
Table A.1 gives an overview of corresponding concepts between systems in general, Petri nets, reachability graphs and concepts of dependability:

Table A.1 – Corresponding concepts in systems, Petri nets, reachability graphs and dependability

Aspect	System	Petri net	Reachability graph	Dependability
Dynamic	Event	Transition	Arc	For example: Failure events or error handling events
Static	Local state	Place		Local state
	Global state	Marking = set of marked places	Node	Global state (e.g. maintenance, hazard)
	Aggregated global state	Set of markings	Set of nodes	Set of global states (e.g. available, safe)

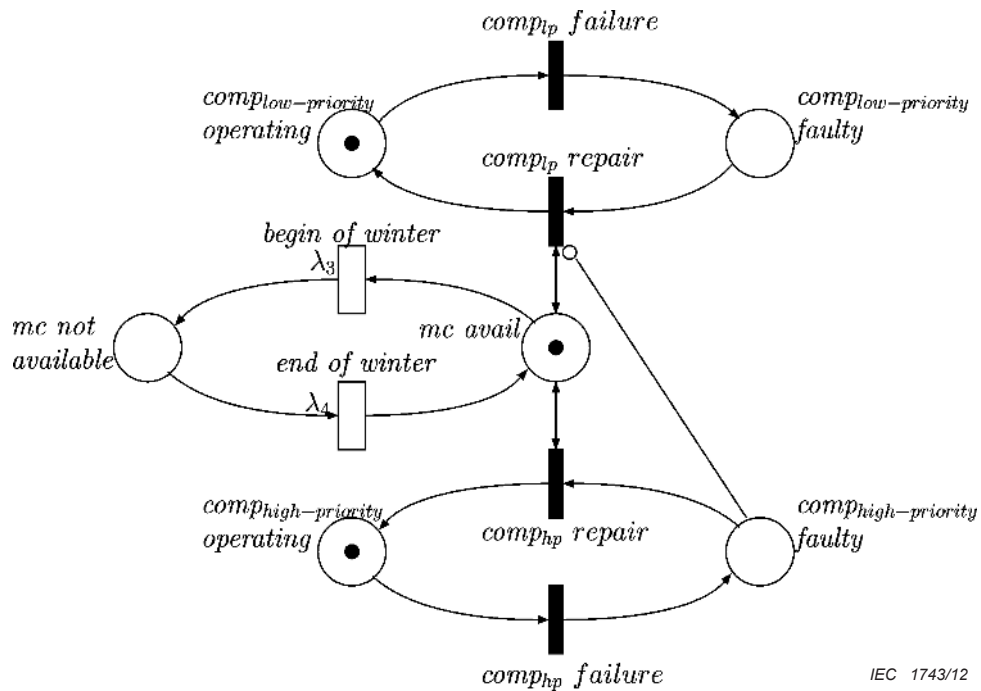
Example

In the Petri net in Figure A.11 transition ‘comp_{lp} repair’ (abbrev. for ‘component_{low priority} repair’) is enabled, because the place ‘comp_{low-priority} faulty’ is marked, maintenance crews are available (at least one crew is needed to repair this component) and the ‘comp_{high-priority}’ is not faulty. In addition, transition ‘comp_{hp} failure’ (abbrev. for ‘component_{high priority} failure’) is enabled due to the fulfilment of condition ‘comp_{high-priority} operating’.



IEC 1742/12

Figure A.11 – Transitions ‘comp_{lp} repair’ and ‘comp_{hp} failure’ are enabled



IEC 1743/12

Figure A.12 – Marking after firing of transition ‘comp_{ip} repair’

Firing of ‘comp_{ip} repair’ absorbs one token from place ‘comp_{low-priority} faulty’ and produces one token on place ‘comp_{low-priority} operating’. As places ‘comp_{high-priority} faulty’ and ‘maintenance-crew available’ are connected with transition ‘comp_{ip} repair’ by test and inhibitor arcs, respectively, their marking is not changed (see Figure A.12).

Note the behaviour of the net in another state: if the component with the high priority fails while the component with the low priority is under repair, then

- the repair of the low priority component is suspended,
- the repair of the high priority component starts,
- the repair of the low priority component is restarted after the repair of the high priority component is finished.

Modelling such ‘suspended’ events by analytical calculations is very difficult, whereas Monte Carlo simulation enables such models to be analysed very easily.

A.2 Timed Petri nets

A.2.1 Introductory remark

For applications in dependability, it is also useful to model temporal aspects. For example, the time that a system is up or down is represented by the time that the net is in the corresponding marking. On the other hand, the delays after which states change are attributed to transitions. Considering time, both deterministic and stochastic behaviour can be distinguished. These two categories can be represented by timed Petri nets with deterministic time parameters (for example deterministic durations of events) and stochastic timed parameters (for example exponential functions with corresponding rates) on their transitions (for stochastic timed PNs see [3] and [16]). In all cases, the transition properties are portrayed by various labels or supplementary conditions.

A.2.2 Specific transitions for timed low-level Petri nets

In timed PN, both untimed as well as timed transitions may be used. In principle, for timed transitions the same firing rule holds as for untimed transitions (see the above-mentioned untimed PN). A timed transition shall be enabled for a specific time duration. This duration may be deterministic or stochastic, depending on the transition-specific distribution function (CDF) and on corresponding parameters. After this duration has elapsed, the transition is allowed to fire. Table 2 shows the commonly used transitions in timed PNs.

Together with the specific type of timed transition, a time parameter shall specify the deterministic firing duration, the (constant) firing rate or the probability distribution with its parameters.

Note that the use of the Dirac distribution $\delta(d)$ for deterministic delays d allows encompassing both, deterministic and stochastic transitions within the same framework ($\delta(0)$ allows encompassing untimed and timed transitions). Nevertheless, it is often useful to distinguish the various kinds of behaviour because they correspond to events differing in their nature.

A.2.3 Dynamics in timed low-level Petri nets

In timed Petri nets, the system dynamics is also modelled by the change of progress of markings which is represented by its corresponding reachability graph (see e.g. Figure A.10). According to the different transition rates or stochastic distributions, their state-transition arcs will be annotated by their specific time symbol. Each global state which models a certain dependability-related state is attributed by a certain probability which results from the transition's temporal behaviour, e.g. its stochastic firing. It has been proved that any finite and marked stochastic PN is isomorphic to a discrete space Markov chain [17] provided that all events are exponentially distributed.

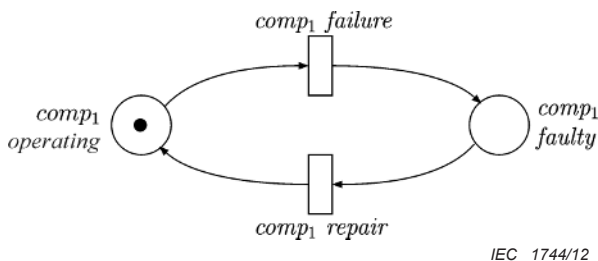


Figure A.13 – A timed PN with two exponentially distributed timed transitions

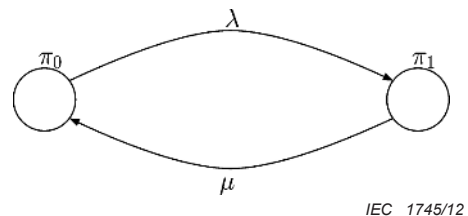
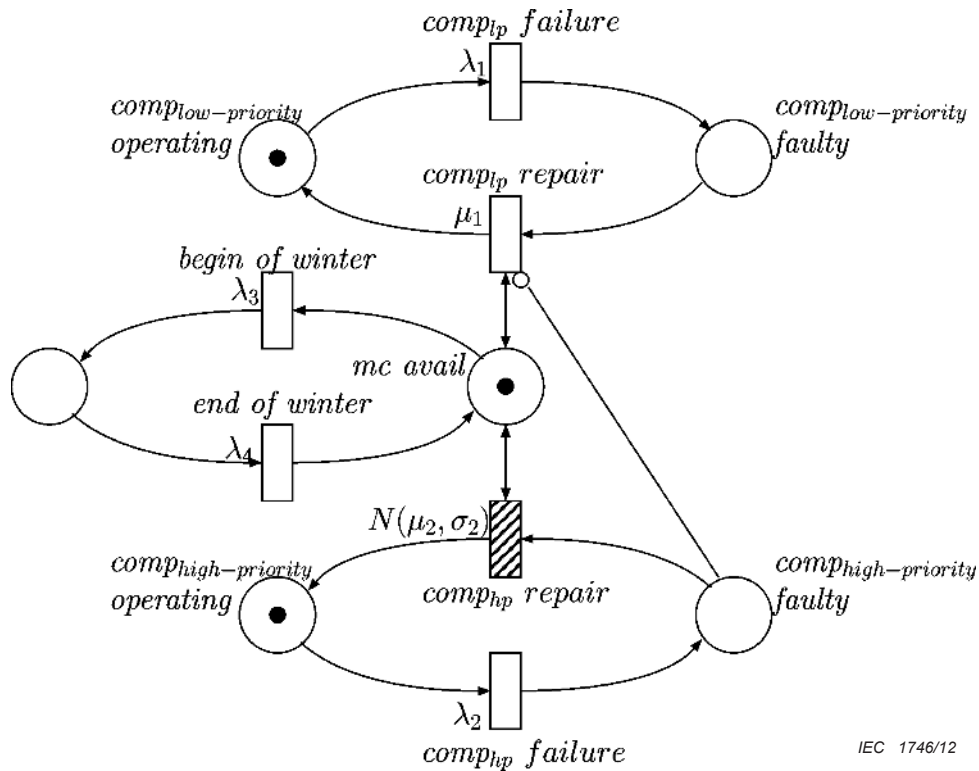


Figure A.14 – The corresponding stochastic reachability graph

In Figure A.13, the transitions are attributed with their transition rates. In Figure A.14, the global states are named π_0 and π_1 , respectively.

Example



IEC 1746/12

Figure A.15 – Petri net with timed transitions

In Figure A.15 the transition ‘*comp_{ip} failure*’ fires with rate λ_1 , i.e. once this component is in its operating state (denoted as *comp_{low-priority} operating*), it remains there for an exponentially distributed time. If *comp_{hp}* is in its faulty state, it remains there for a normal distributed time, specified with the parameters μ_2 (mean) and σ_2 (standard deviation). It should be noted that here the truncated normal law with a restricted support to $(0, \infty)$ for transition $N(\mu_2, \sigma_2)$ is presumed. In addition, the same remarks on suspended events as for the nets in Figure A.11 and A.12 hold.

A.2.4 Different classes of timed Petri nets

There are many subclasses of stochastic PN (SPN). In a first classification one can say that the class depends on the choices of the firing time distributions which have significant influence on the possible analyses.

The following model classes are common in the literature (e.g. [3]):

- generalized stochastic Petri nets (GSPN): all timed transitions have an exponentially distributed firing time;
- Markovian SPN (MSPN): SPNs for which the underlying stochastic process is a Markov chain. This is the case if all timed transitions have an exponentially distributed firing time or if all timed transitions have a geometrically distributed firing time (i.e. memoryless and discrete time). The first possibility corresponds to GSPNs;
- deterministic and stochastic Petri nets (DSPNs): the timed transitions are either exponential or deterministic and the deterministic transitions are mutually exclusive and have a special preemption policy;
- Markov regenerative stochastic Petri nets (MRSPNs): SPNs for which the underlying stochastic process is a Markov regenerative process. A subclass, also known as extended

DSPN, is given by SPNs where the timed transitions are either exponential or general and the general transitions are mutually exclusive and have a special preemption policy;

- non-Markovian stochastic Petri nets: any SPN which is not Markovian.

A.3 Methods to analyse Petri nets

A.3.1 General

In general, there are two principally different analysis tasks:

- a) qualitative tasks deal with questions concerning possibilities, such as “Is it possible that a certain state can be reached?” or “Is it possible that a certain event can take place?”;
- b) quantitative tasks deal with questions concerning (among others) probabilities, such as “What is the probability that a certain state is reached?” or “What is the probability that a certain event takes place?”.

Analysis tasks can therefore be divided into qualitative and quantitative tasks.

A.3.2 Qualitative analysis

Qualitative analyses can be divided into structural and dynamic analyses;

- structural analyses only take the structure of the Petri net into account, the RG is not considered. Therefore, these analyses are independent of the initial marking. The advantage of these analyses is that results hold for every arbitrary initial marking. The disadvantage is that such results are often quite general. Invariants, deadlocks and traps are well known structural properties of Petri nets [16];
- dynamic analyses take into account the RG or a subset of it, e.g. a (shortest) sequence or a set of sequences of a Petri net. As the RG is based on a specific initial marking, these results depend as well on the initial marking. The advantage of these analyses is that if the RG can be generated and handled, every qualitative question can be answered. The disadvantage is that it is often impossible to create the RG due to its size. Dynamic analyses identify e.g. if hazardous or accidental states might occur [18].

A.3.3 Quantitative analysis

A.3.3.1 General

Often, system dependability features and their measures such as steady-state or transient probability of system operability become the focus of interest. Many of the methods and algorithms that are necessary in order to quantitatively analyse systems have their foundations in probability theory. Of course, one has to specify the relevant probability distributions before the analyses can be carried out. If there are only exponential distributions in the system’s model, it is a ‘homogeneous Markovian’ model. To solve models of this type, all the approaches concerning analyses of Markov chains can be used. The method for analysing industrial-sized models is described e.g. in [12]. In addition, PNs have proven to be very efficient for safety calculations of safety related systems (SIL-calculation) such as probability of failure on demand (i.e. the average unavailability) and probability of failure per hour (i.e. the average failure frequency).

A.3.3.2 Analyses of Markovian models

In order to use the analysis methods for CTMCs (continuous time markov chain), a stochastic Petri net is mapped to a CTMC; to perform this mapping it is necessary that the stochastic PN is a GSPN (see A.2.4, [3]). Two kinds of solutions to Markov processes ([19]) are of interest: transient and steady-state. The transient solution is obtained by solving the “Kolmogorov differential equation” and the steady-state solution is obtained by solving a linear system of equations. Closed-form analytical results are possible for either highly structured Markov graphs or very small Markov graphs. In most other cases, numerical solution techniques shall be used.

Markov processes may be used to assess

- the probability of the states (time-dependent and asymptotic),
- the cumulated time spent in the states (e.g. for production availability purpose).

In the specific domain of production availability problems ‘multi-states’ Markov processes are used, when dealing with periodically tested safety systems ‘multi-phase’ Markov processes are often used.

There is plenty of literature on solving Markovian models (see [18] and [19]).

A.3.3.3 Analyses of non-Markovian models

When the assumption of exponential distribution is relaxed, the underlying models can be solved by various techniques:

- in Markov renewal theory, processes are considered at certain time instants where the processes are memoryless. It is said that a process regenerates in these instants and that another process is embedded in these instants. It is possible to express the state equations for the embedded processes and to derive the solutions of the actual process from them [3];
- the Monte Carlo simulation method is a methodology for obtaining estimations of the solution of mathematical problems by means of random numbers. This method relies on repeated computation with random variables. The advantage of this approach comes from the fact that it allows taking the many phenomena that can occur realistically into account, without additional complication in the solution procedure. The principal disadvantage in former times was the use of relevant calculation times, which diverge with the required accuracy. Nowadays, one can say that this argument is obsolete (e.g. [12]). In addition, the MC simulation always provides the accuracy of the results (confidence interval). This is not the case when truncated or aggregated Markov models are handled.

A.3.3.4 Reward functions

For stochastic processes, ‘rate rewards’ are values which are accumulated when the model spends time in a state and ‘impulse rewards’ (often: ‘assertions’) are values obtained when transitions fire in certain markings. In general, rate rewards can be calculated on the basis of



- statistics concerning the different states of the system,
- statistics concerning the variables of the system,
- the time spent by tokens in the various locations,
- and others.

The computation of impulse rewards on the other hand is based on the transitions’ firing frequencies ([3]).

These concepts make it possible to easily model the costs and rewards related to failure and operating states, respectively. Furthermore, costs of repair events can easily be taken into account. This is useful, for example, when dealing with production availability calculations. An example of the application of reward functions in the dependability domain can be found in Annex D.

The graphical representations of a place and a transition with rewards are given in Table A.2.

Table A.2 – Place and transition with rewards

Identifier <i>rr</i> 	Identifier <i>ir</i> 
Place with rate reward	Transition (exponentially distributed) with impulse reward

Annex B (informative)

Availability with redundancy m-out-of-n

B.1 Local and global states

The ability of any item to perform a function can be modelled by a Petri net with a state-transition circle to express its availability, e.g. states when an item is operating or faulty (see Figure A.1).

The resulting system availability model shows the combinatorial sets of the item's local availability by means of global states (see Figures B.1 and B.2 for a system consisting of two items and no connections between the items and Figures B.3 and B.4 for a system consisting of three items without any connection). These will be derived by constructing the reachability graph from this entire net; here, all global states of the system are represented.

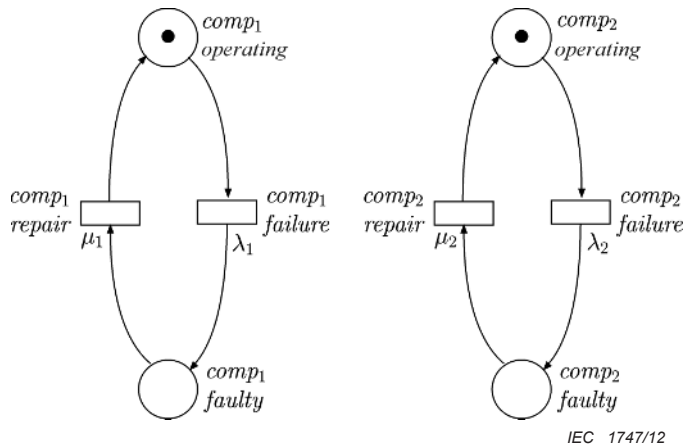


Figure B.1 – Two individual item availability nets with specific failure- and repair-rates

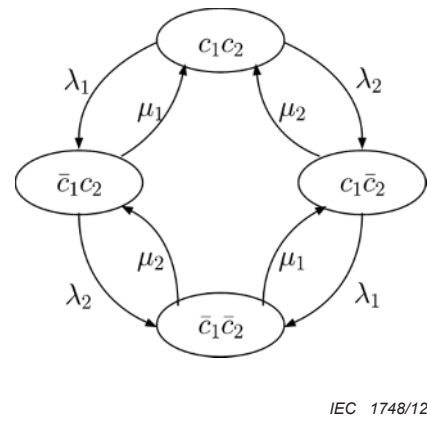


Figure B.2 – Stochastic reachability graph corresponding to Figure B.1 with global states (as an abbreviation \bar{c}_1 is used for “*comp₁ faulty*”)

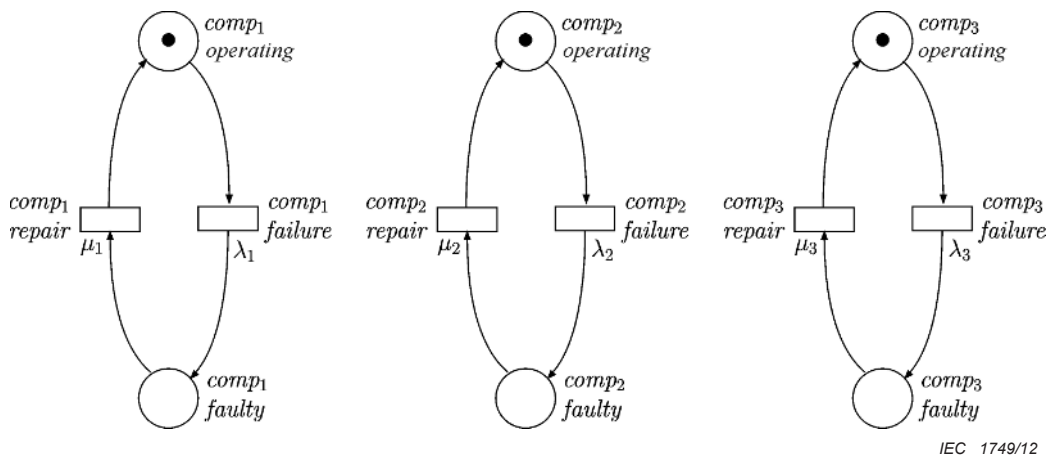


Figure B.3 – Three individual item availability nets with specific failure rates and repair rates

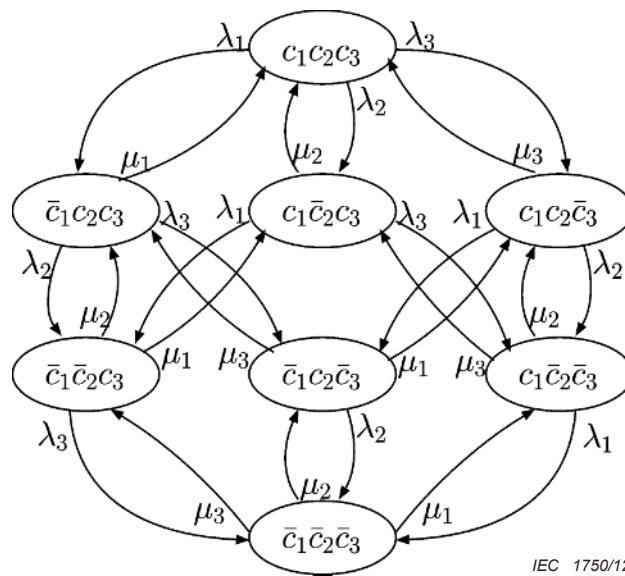
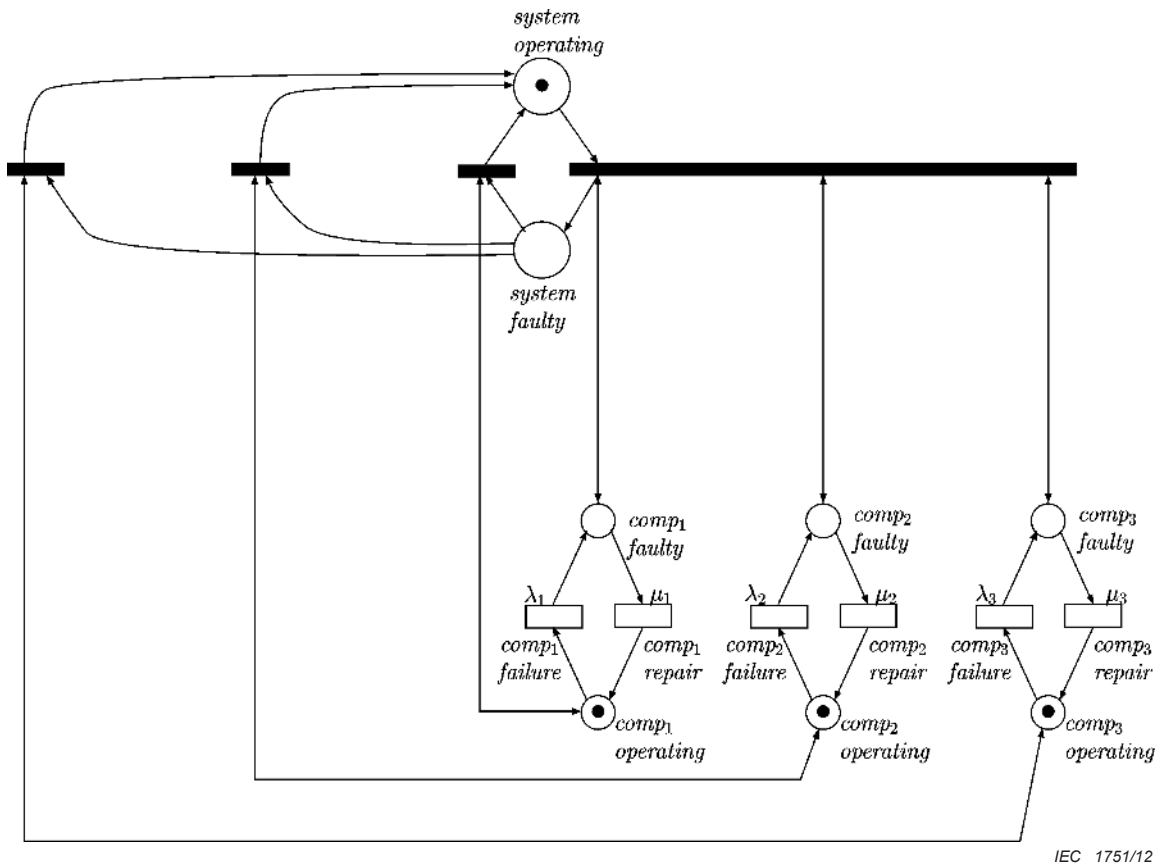


Figure B.4 – Stochastic reachability graph corresponding to Figure B.3 with global states (as an abbreviation \bar{c}_1 is used for ‘comp₁ faulty’)

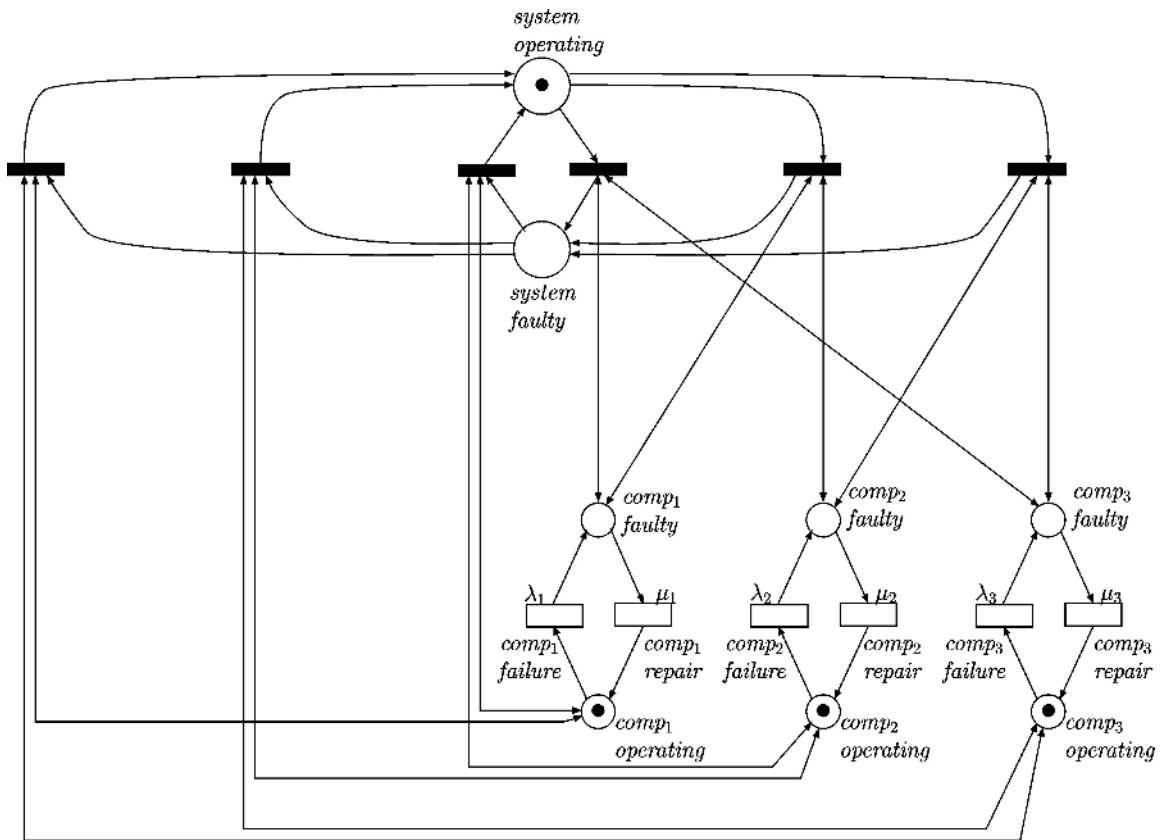
B.2 Global states and system structure

For the implementation of a complex functional system structure which will be performed by several connected items (which itself perform sub-functions), corresponding instances of the basic modelling concept shall be connected taking into consideration the whole system structure, e.g. chain, redundancy. According to this logical structure, the reachability graph shows implicitly all the global states of the system’s availability and unavailability. See Figures B.5, B.6 and B.7 for the dependability structures modelling 1-out-of-3, 2-out-of-3 and 3-out-of-3 systems, respectively. An overview of largeness avoidance and largeness tolerance techniques can be found in [20] as well as further model construction technologies.



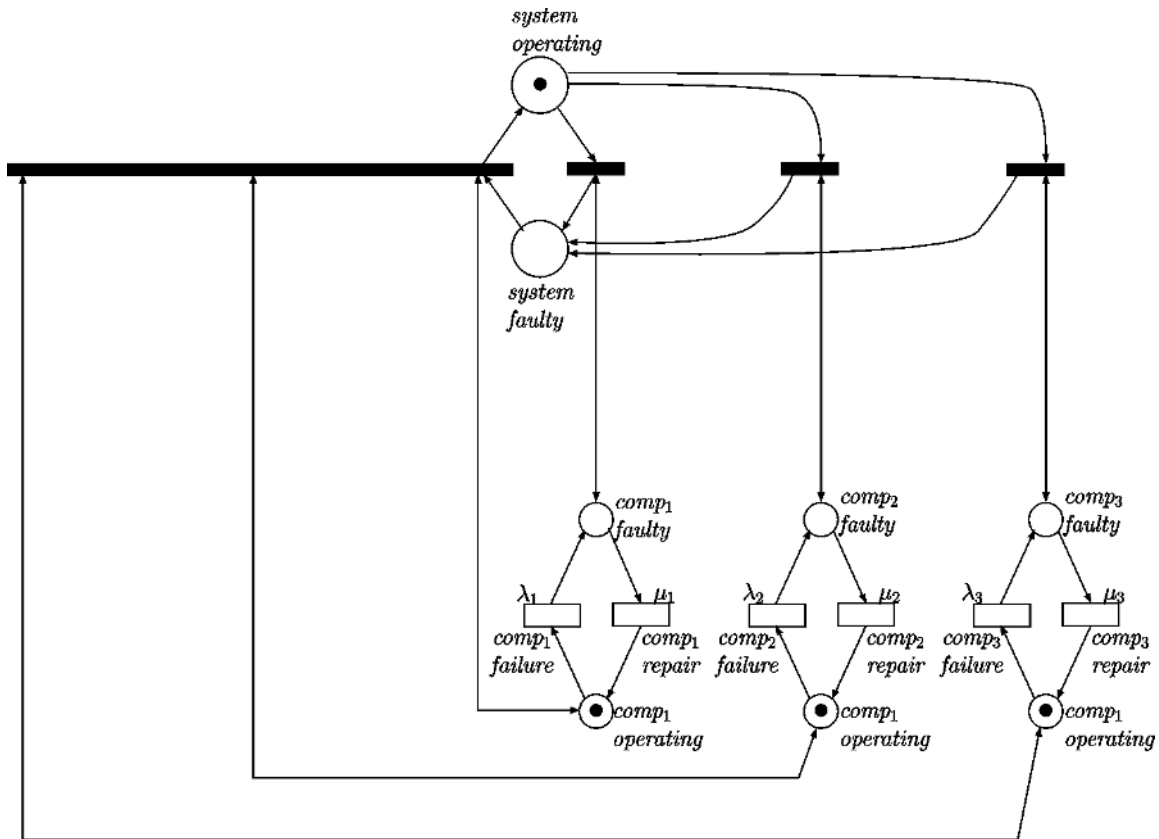
IEC 1751/12

Figure B.5 – Specifically connected 1-out-of-3 availability net



IEC 1752/12

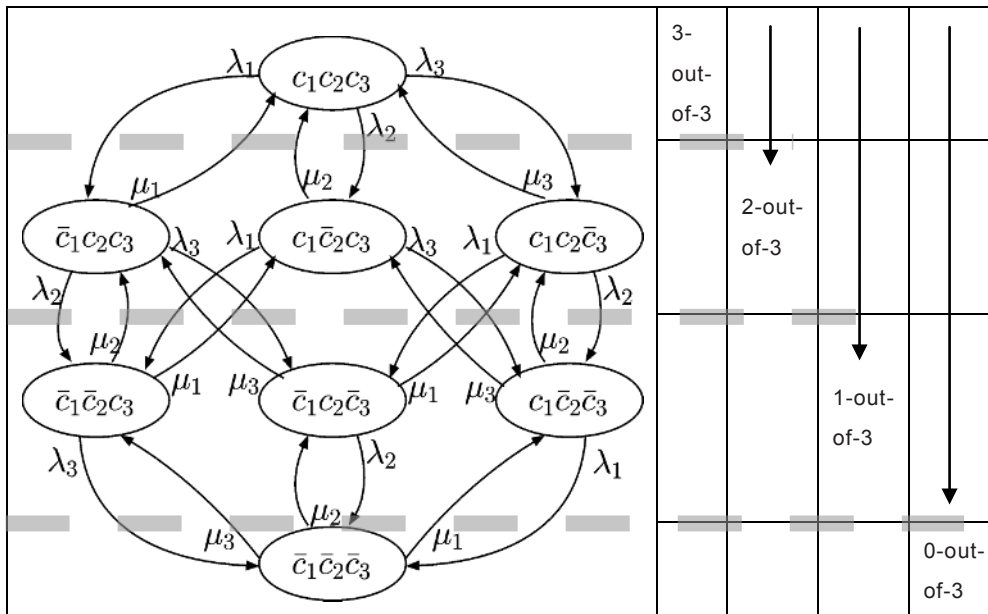
Figure B.6 – Specifically connected 2-out-of-3 availability net



IEC 1753/12

Figure B.7 – Specifically connected 3-out-of-3 availability net

The states of the corresponding stochastic reachability graph can be classified correspondingly – see Figure B.8. For example, in a 3/3-system, the system is operating only when component₁, component₂ and component₃ are operating; in a 2/3 system, there exist four possible states, in which the system is operating.



IEC 1754/12

Figure B.8 – Stochastic reachability graph with system specific operating states

Concerning reliability, the corresponding systems can be modelled as shown in Figures B.9, B.11 and B.13. The corresponding reachability graphs are presented in Figures B.10, B.12 and B.14, respectively.

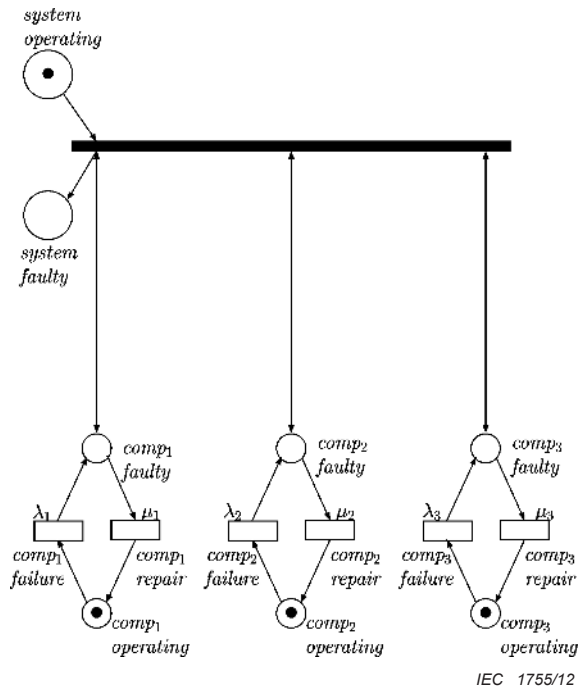


Figure B.9 – Specifically connected 1-out-of-3 reliability net

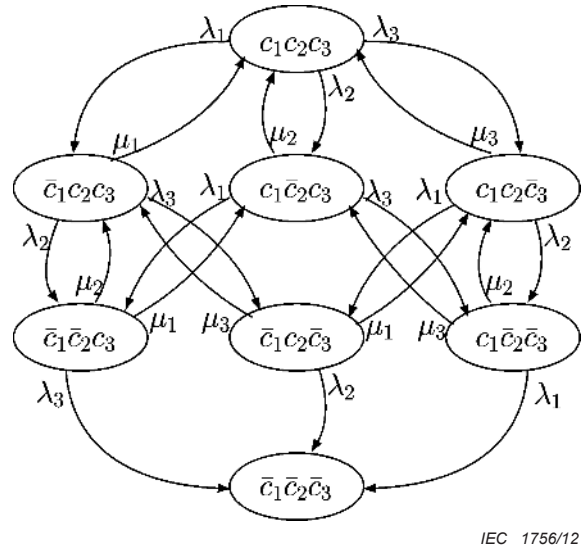


Figure B.10 – Reachability graph for the net in Figure B.9

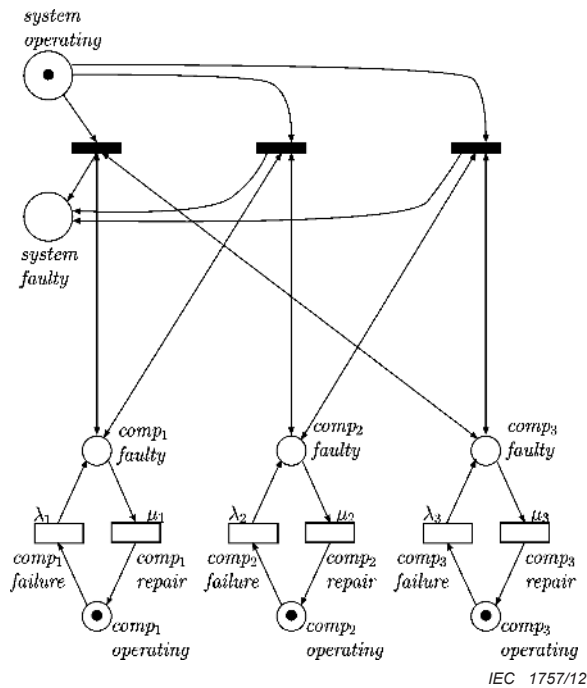


Figure B.11 – Specifically connected 2-out-of-3 reliability net

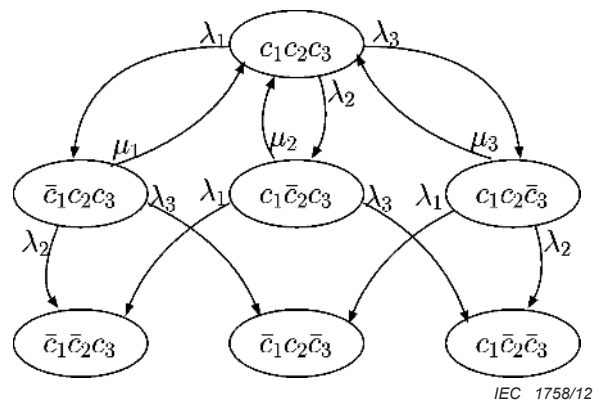


Figure B.12 – Reachability graph for the net in Figure B.11

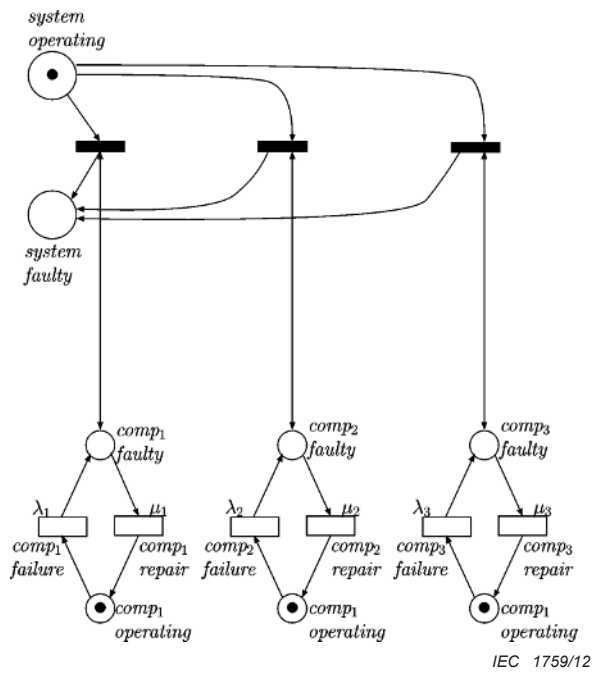


Figure B.13 – Specifically connected 3-out-of-3 reliability net

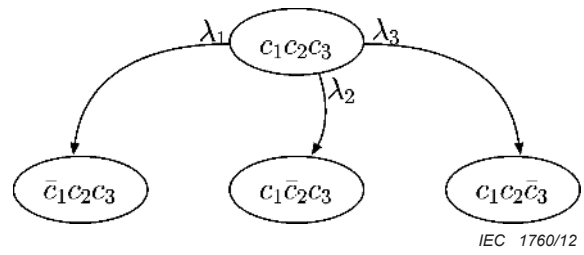


Figure B.14 – Reachability graph for the net in Figure B.13

Annex C (informative)

Abstract example

C.1 Local, global and aggregated global states

With respect to dependability, the Petri net and corresponding reachability graph can represent all its different features, i.e. availability, maintainability, etc.

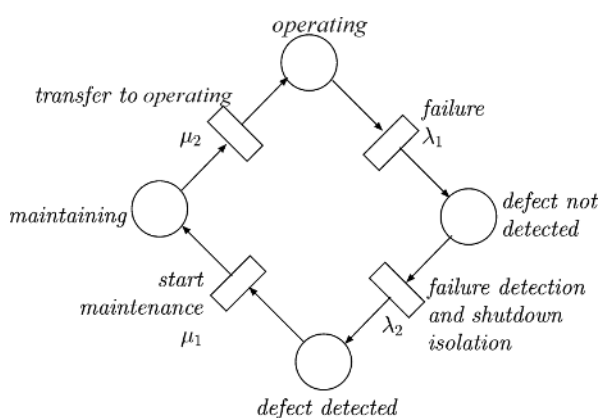
With regard to availability and maintainability, the different conditions of an item of a system to perform a function can be modelled in more detail by an extended circular Petri net (see Figure C.1) which incorporates the item's different states. These are, for example:

- operating;
- defect, but not detected as defect i.e assumed to be operating;
- detected defect;
- maintained by repair or replacement or other means of maintenance.

This can be done together with their four transitions:

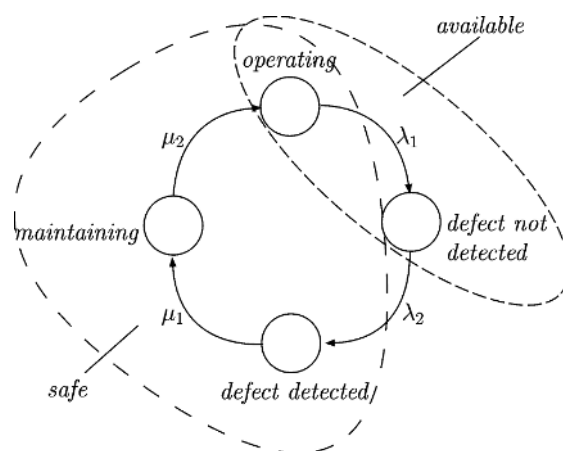
- failure event;
- failure detection and stop or shut down;
- start maintenance;
- transfer to operating state.

Note that the last three places and their interconnected transitions could be condensed to a superplace which equals the one “comp₁faulty” place in Figure A.1. The resulting reachability graph has a similar simple structure. It shows four global states and their probabilities, as well as the single state transitions with their rates. With respect to availability and safety, some global states can be condensed to a single aggregated global state which represents all states of available or safe, as shown in Figure C.2.



IEC 1761/12

Figure C.1 – Individual availability net



IEC 1762/12

Figure C.2 – Stochastic availability graph of the net in Figure C.1 with its global states and aggregated global states according to availability and safety

Considering the features of availability and safety, numerical values of their measurements can clearly be represented in an availability-safety orthogonal coordinate system. This shall be scaled by a logarithmic measure of probability of unavailability or lack of safety, called the probability potential pA of availability, and pS of safety, respectively because availability and safety probability generally approximate the numerical value one:

$$pA = -\log(1 - A) \quad A = \sum_{i \in A} p_i \tag{C.1}$$

where A is the probability to be in a state of the set of all states where the system is available.

$$pS = -\log(1 - S) \quad S = \sum_{j \in S} p_j \tag{C.2}$$

where S is the probability to be in a state of set of all states where the system is safe.

For example, let $A = 0,999\ 9$, i.e. $(1-A) = 0,000\ 1$ and $-\log(1-A) = 4$. For $A' = 0,999\ 99$, $pA = -\log(1-A') = 5$, i.e. pA correlates with A . The same holds for S and pS , respectively.

C.2 Availability, reliability, system function and hierarchization

Based on the definition of reliability, the Petri net model includes the required function as a state-transition-state consequence. The availability of the component itself to perform the required function will be modelled by a separate reliability state-transition circle to express its operating and complementary faulty state (see Figure A.1).

Both subnets are connected via test arcs from the operating state to the performing function (see Figure C.3).

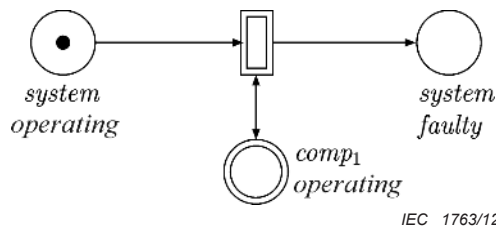


Figure C.3 – Basic reliability and function modelling concept

This basic modelling concept consists of an abstract logical function which is performed by an item named ‘resource’, which itself provides a functionality, i.e. the ability to perform at least the required function. This basic modelling concept integrates the functional capability and reliability behaviour of an item (resource).

In Figure C.4 the supertransitions hide the specific logical structure specifying the n -out-of-3 connection. The ‘ n ’ here depends on the net that is hidden by the supertransitions. In addition, in Figure C.5 the state-transition circles of each single component has also been hidden by superplaces. That means supernodes make it possible to hide specific modelling details and allow the abstraction of specific implementations.

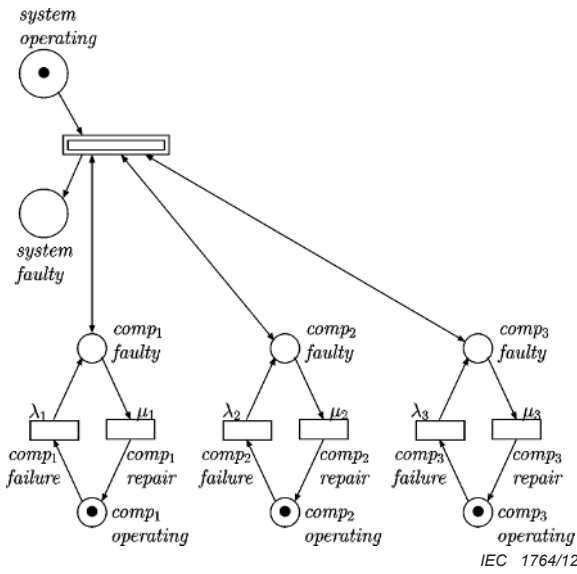


Figure C.4 – General hierarchical net with supertransitions to model reliability

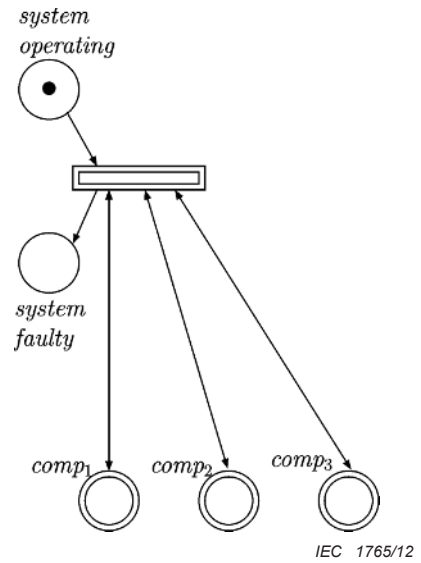


Figure C.5 – General hierarchical net with supertransitions and superplaces

The corresponding availability models can be found in Figure C.6 and C.7.

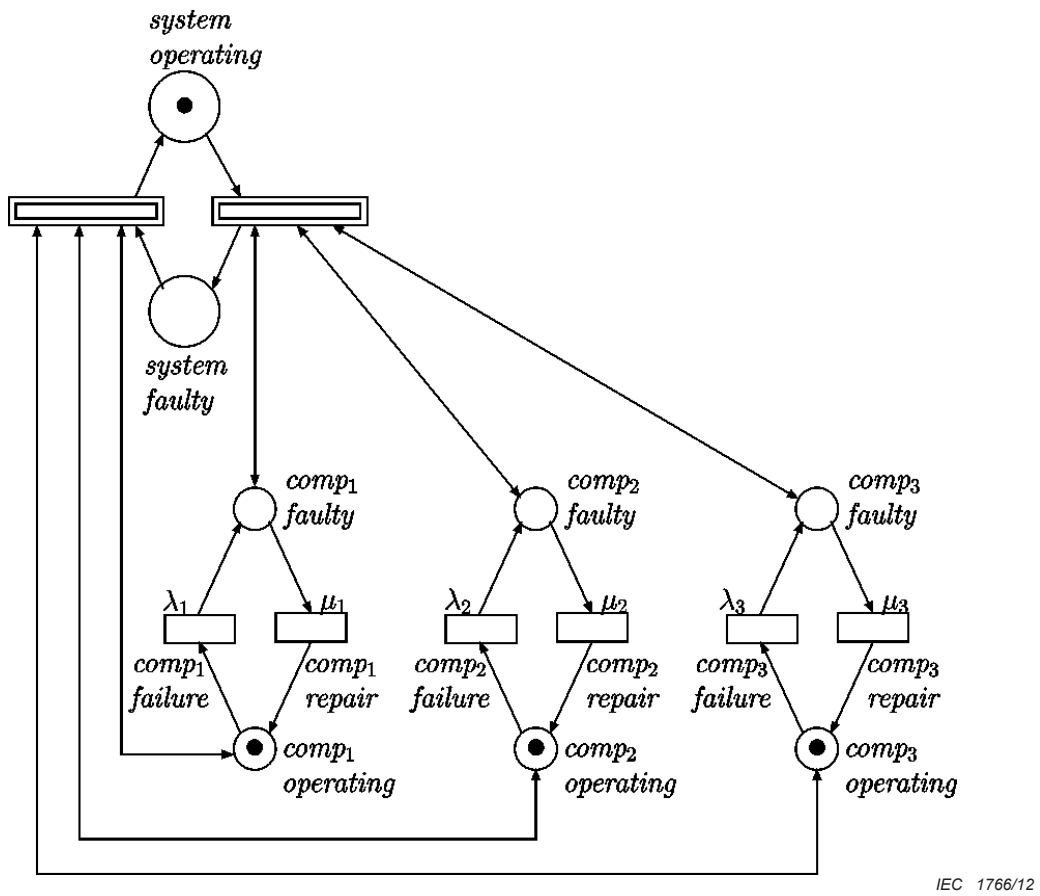


Figure C.6 – General hierarchical net with supertransitions to model availability

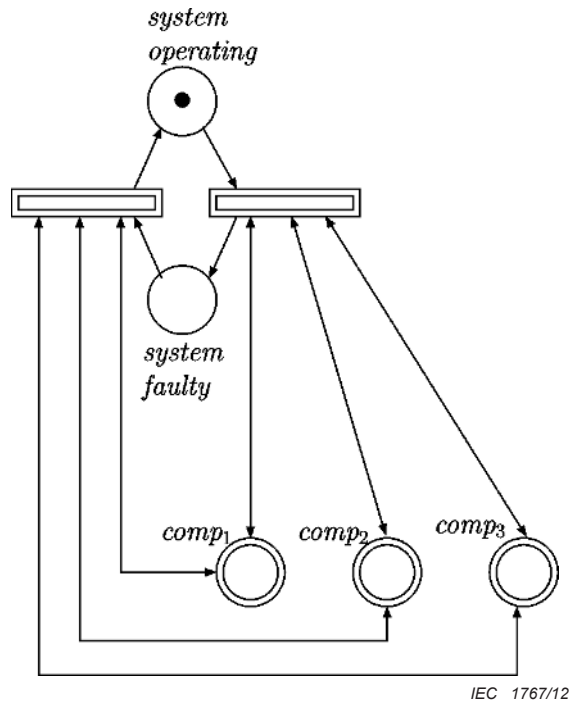


Figure C.7 – General hierarchical net with supertransitions and superplaces

Annex D
(informative)

Modelling typical dependability concepts

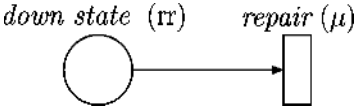
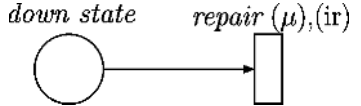
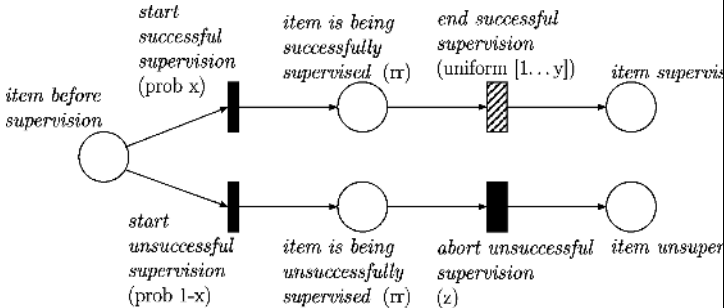
Table D.1 shows how general dependability concepts are modelled with PN structures.

Table D.1 – Dependability concepts modelled with PN structures

Dependability concept	PN modelling solution
Failure with constant failure rate λ (leading to exponentially distributed times to failure)	<p><i>up state</i> <i>failure</i> (λ)</p>
Repair or recovery with constant rate μ leading to exponentially distributed repair/recovery times)	<p><i>down state</i> <i>repair</i> (μ)</p>
Repair or recovery with a fixed repair time of n time units)	<p><i>down state</i> <i>repair</i> (n hours)</p>
Repair or recovery (with a truncated normal distributed repair time with a mean of x and a standard deviation of y)	<p><i>down state</i> <i>repair</i> ($N(x, y)$)</p>
Maintainability (for the maintenance action 'supervision', probability x % for successful finalization, with $0 \leq x \leq 1$)	

Table D.2 suggests how to model costs of specific states and events. In this context one uses the PN concepts of rewards: 'rate rewards' (rr) and 'impulse rewards' (ir), see Table A.2. It should be noted that here the truncated normal law with a restricted support to $[0, \infty]$ for transition $N(x, y)$ is presumed.

Table D.2 – Modelling costs of states and events

Type of cost	PN modelling solution
Cost of failure (costs are proportional to the cumulative time spent in down-state)	
Cost of repair or recovery (costs are proportional to the number of repairs)	
Cost of maintainability (for the maintenance action 'supervision', probability x % ($0 \leq x \leq 1$) for successful finalization and a supervision time uniformly distributed in the interval $[1...y]$; accumulated supervision costs arise in any case)	

Annex E (informative)

Level-crossing example

E.1 Introductory remark

To illustrate the application of Petri nets for dependability, the example of modelling a protected level crossing (with barriers) has been chosen. In this example, the availability of the level crossing to road traffic as well as the risk expressed by fatalities per year shall be determined. Against this background the hazard rate of the level crossing, the intermediate arrival times of cars and trains, as well as the possible behaviour of car drivers arriving at a level crossing are probabilistic parameters of interest.

E.2 Description of main parts and functions of the system

In the first step, the main parts and functions of the system are described by conventional means of description, e.g. textually, with tables, and figures etc. (see 5.2.2).

- a) Figure E.1 shows the assumed topological condition of a particular level crossing. It contains both interacting traffic flows (on rail and road) as well as the protecting equipment controlling the exclusive use of the common part of the transportation path. It is assumed that the system shown has no relations with other systems.

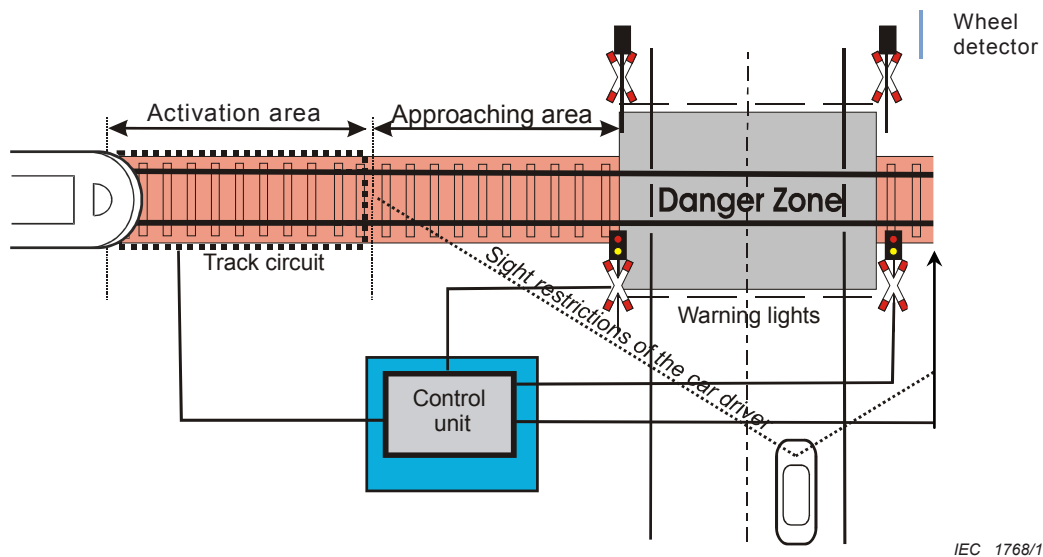


Figure E.1 – Applied example of a level crossing and its protection system

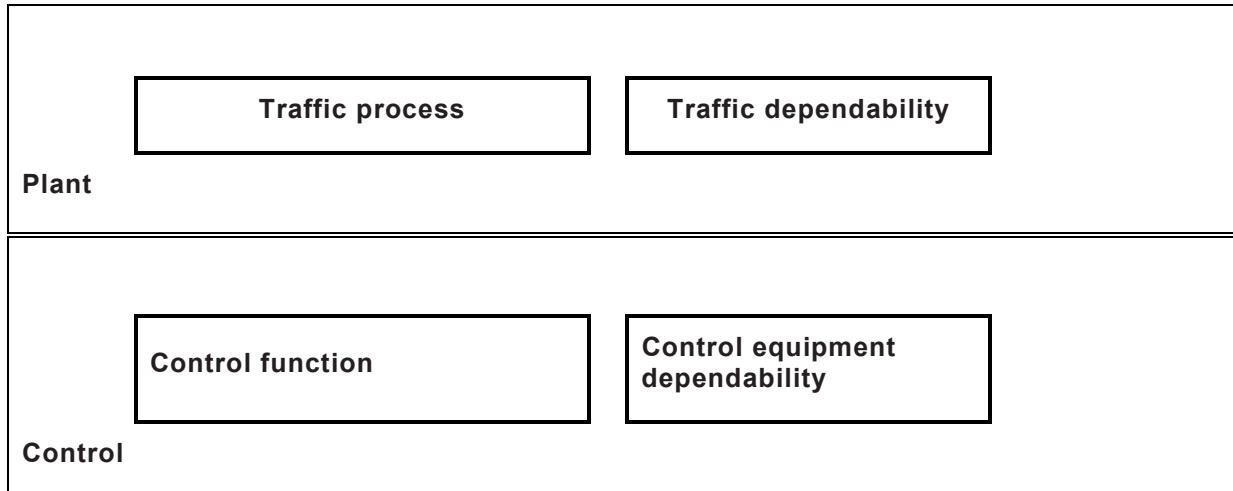
- b) The main parts of the system are the plant, represented by the interacting road and rail traffic, and the control, implemented by the level crossing protection equipment.
- c) The main function of road and rail traffic is the safe transport of persons and goods. Constant speeds of both kinds of vehicle, corresponding to the maximum permitted road and rail speed limits are assumed. The only possible interaction between the traffic flows is given by possible recognition of a rail vehicle by the driver of the road vehicle. In this case, the road vehicle shall be halted. The recognition of road vehicles by the train driver does not lead to any change in train speed.
- d) The main function of the protecting equipment is to warn road vehicle drivers of an approaching train using a visual signal. The equipment must therefore be able to detect a rail vehicle in a defined time (activation time T_{AC} when the train is in activation and approaching areas after which the train will reach the danger zone) which guarantees a

safe passage through the danger zone for any road vehicles which were not able to stop before the danger zone once the warning signal was activated.

E.3 Modelling the structure of the system on the basis of PN submodels

In the second step, the structure of the system is modelled on the basis of PN submodels and their relations, and documenting that model (see 5.2.3).

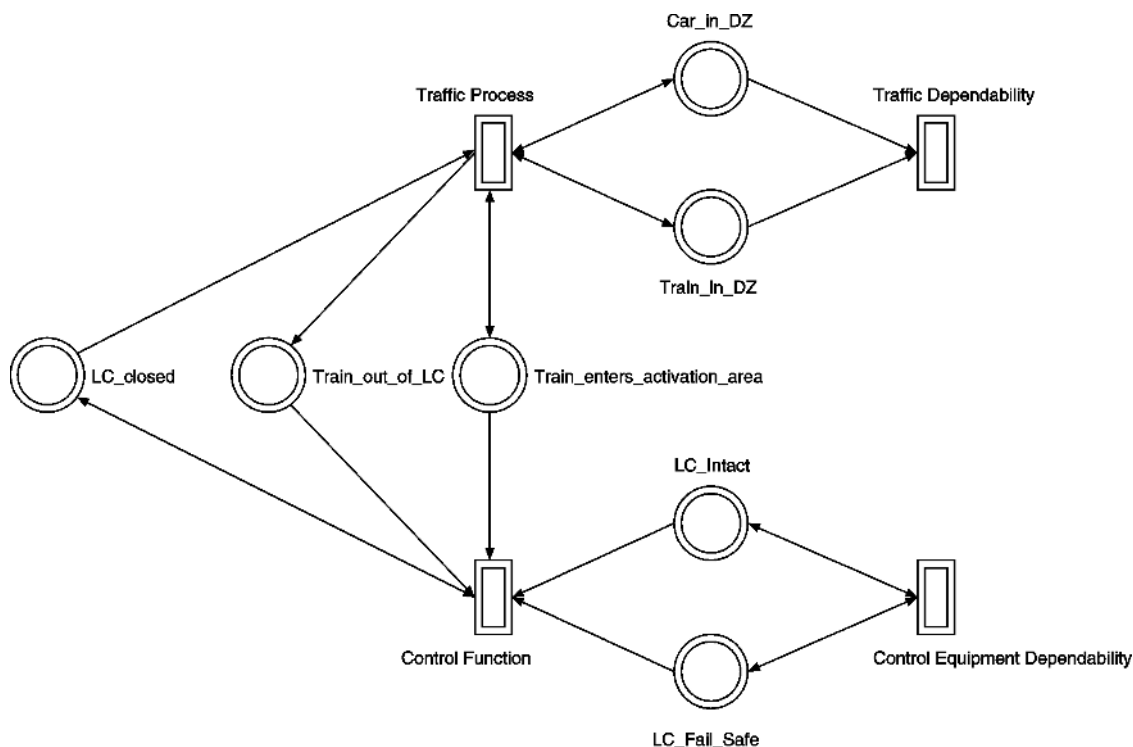
Figure E.2 shows the main model parts to be considered in order to allow the dependability analysis of the traffic processes in the level crossing example.



IEC 1769/12

Figure E.2 – Main parts of the level crossing example model

Figure E.3 shows the corresponding submodels based on the use of supertransitions. This figure reveals the information exchange between the main parts of the model.



IEC 1770/12

Key

LC level crossing
dz danger zone

Figure E.3 – Submodels of the level crossing example model

The model consists of four submodels:

- a) A submodel to specify the traffic process: this submodel specifies the approach and leaving of cars and trains at a level crossing. If a car meets a train in the danger zone, an accident will occur. The purpose of this model is to describe the consequences of the behaviour of different car drivers in terms of probability of an accident. This model does not take any safety measures into account.
- b) A submodel to specify the traffic dependability: here, the possible occurrence of accidents is explicitly modelled. In addition, the procedure of an accident removal is taken into account, i.e. the time until road and railway are cleared and available again.
- c) A submodel to specify the control function: in this subnet, the behaviour of the level-crossing barrier is modelled. Here, failures that would lead to hazardous states are not taken into account. There will only be two local states: 'level crossing open' and 'level crossing closed'. Its behaviour influences, and is in return influenced by, the traffic process.
- d) A submodel to specify the control equipment dependability: here, the dependability of the control function is modelled. As failures are taken into account, one distinguishes between safe-failure and hazardous states. The behaviour of this submodel influences the control function's behaviour.

E.4 Refining the model until the required level of detail is achieved

E.4.1 General

In the third step, the model of step 2 is refined until the required level of detail is achieved and consequently, the refined model is documented (see 5.2.4). One may divide this step by firstly refining the pure structure of the model and secondly specifying the individual parameters to all the nodes of the model.

E.4.2 Refining the structure of the model

Accidents can be seen as consequences of hazardous situations occurring in the traffic process. The model describes this dependence on the basis of the combination of the following four submodels:

- a) traffic flows on the level crossing (LC) in the traffic process submodel;
- b) accident occurrences in the traffic dependability submodel;
- c) LC operations in the control function submodel;
- d) sources of the hazardous influences in the control equipment dependability submodel.

One may start with the traffic process by modelling the “pure” car and train traffic processes, see Figure E.4.

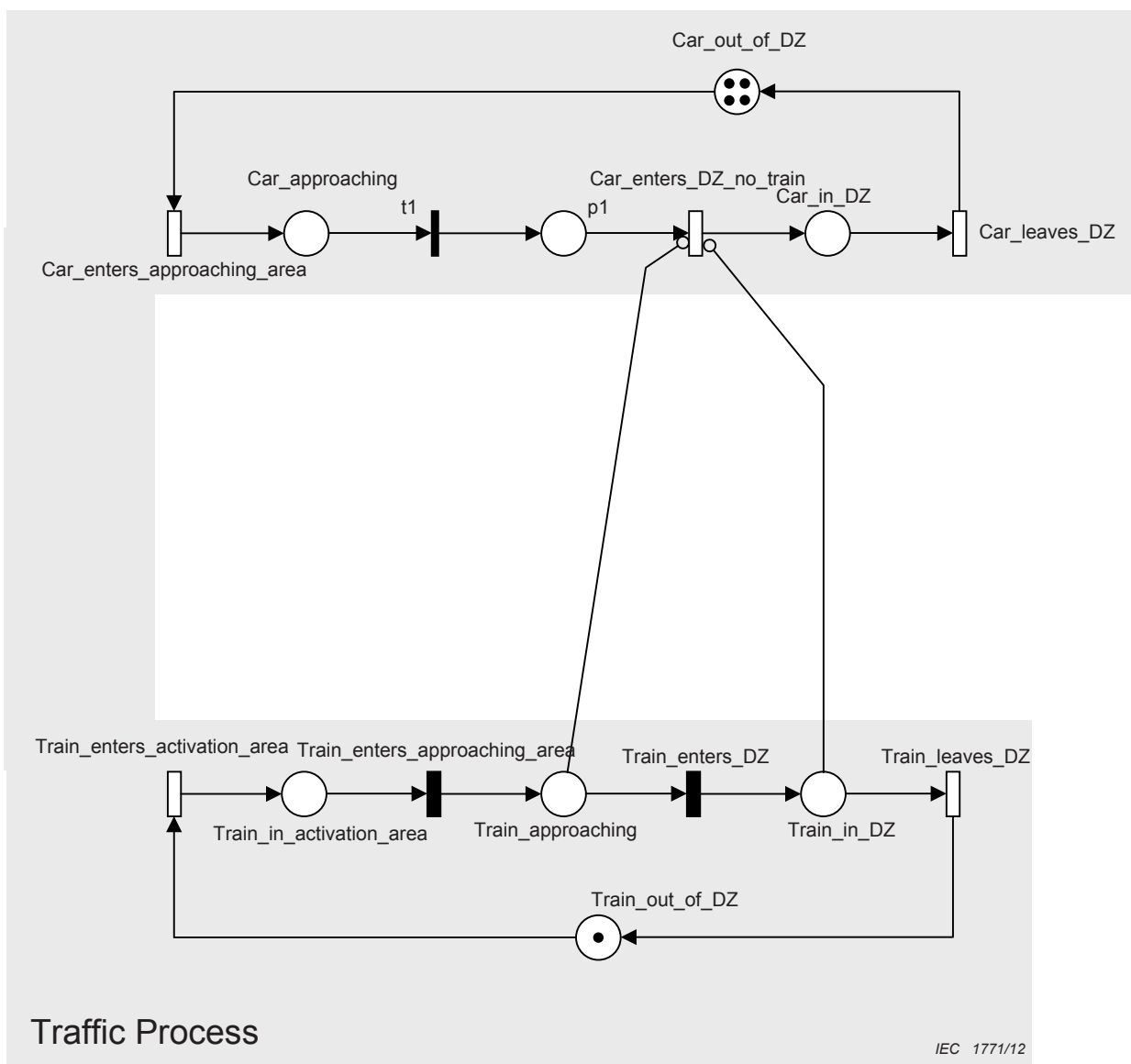


Figure E.4 – PN model of car and train traffic processes

In this submodel the traffic process in an “ideal world” is modelled: all the car drivers only enter the danger zone (DZ) if there is no train approaching or already in the danger zone.

Therefore, no accident is going to happen. In addition, this model does not take into account any control function of the level crossing.

Taking different types of drivers into account requires the “traffic dependability”-submodel. In this submodel, the drivers that enter the danger zone when a train is approaching, as well as the drivers that enter the danger zone even if a train is already in the danger zone, are considered. Taking these two types of drivers into account, accidents may happen. In this model, there is still no control system, i.e. there is no level crossing considered – see Figure E.5.

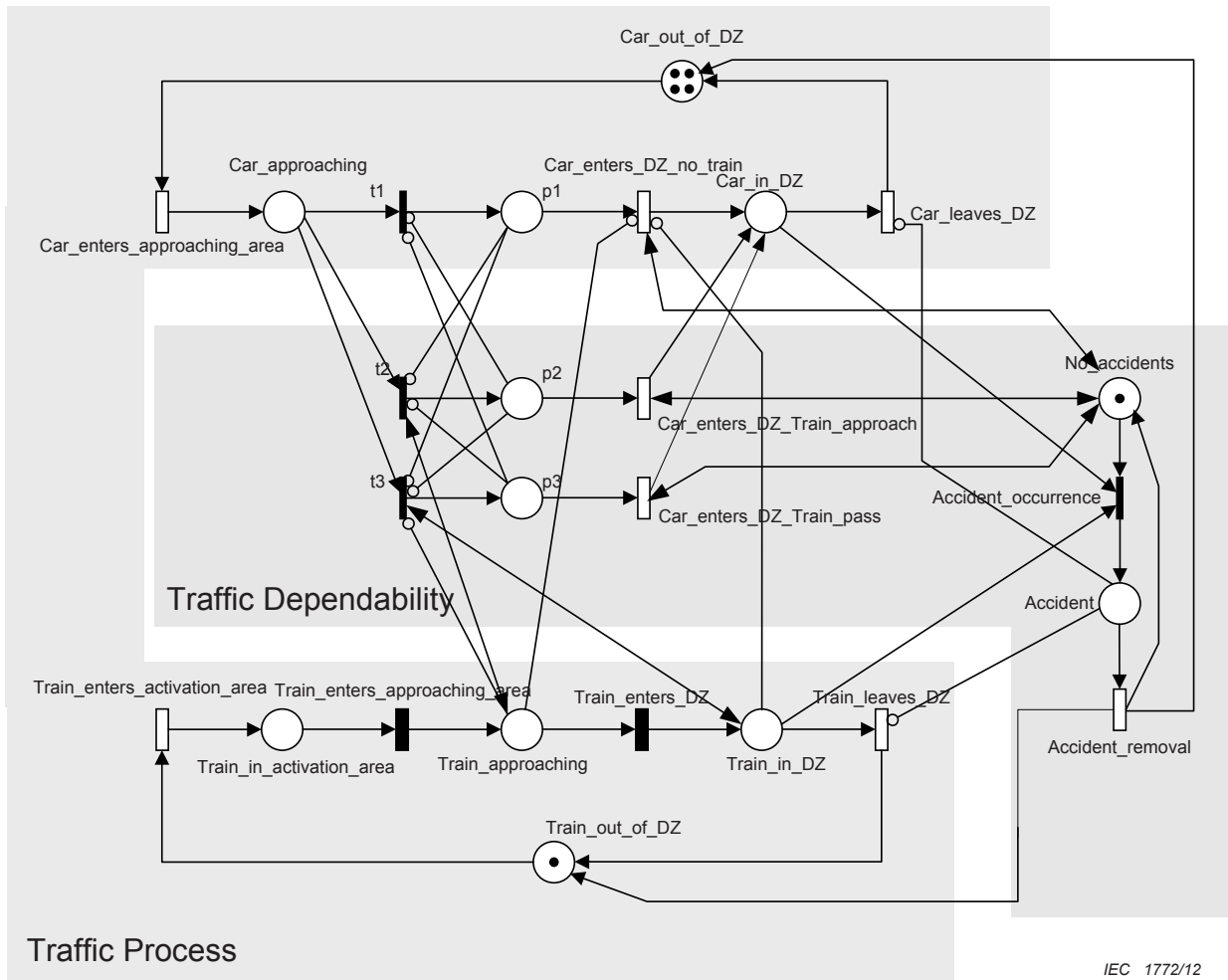
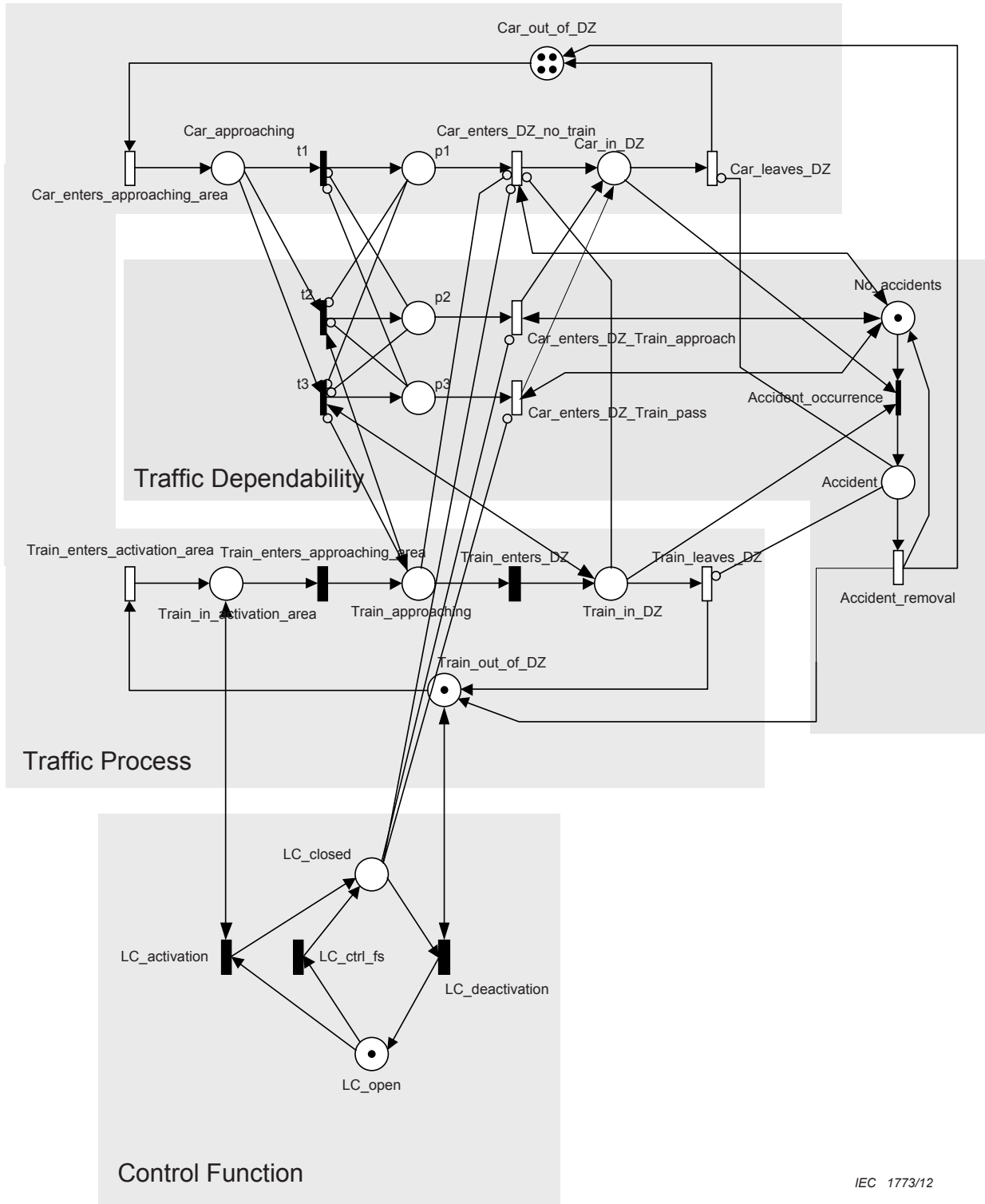


Figure E.5 – PN model of the traffic processes and traffic dependability

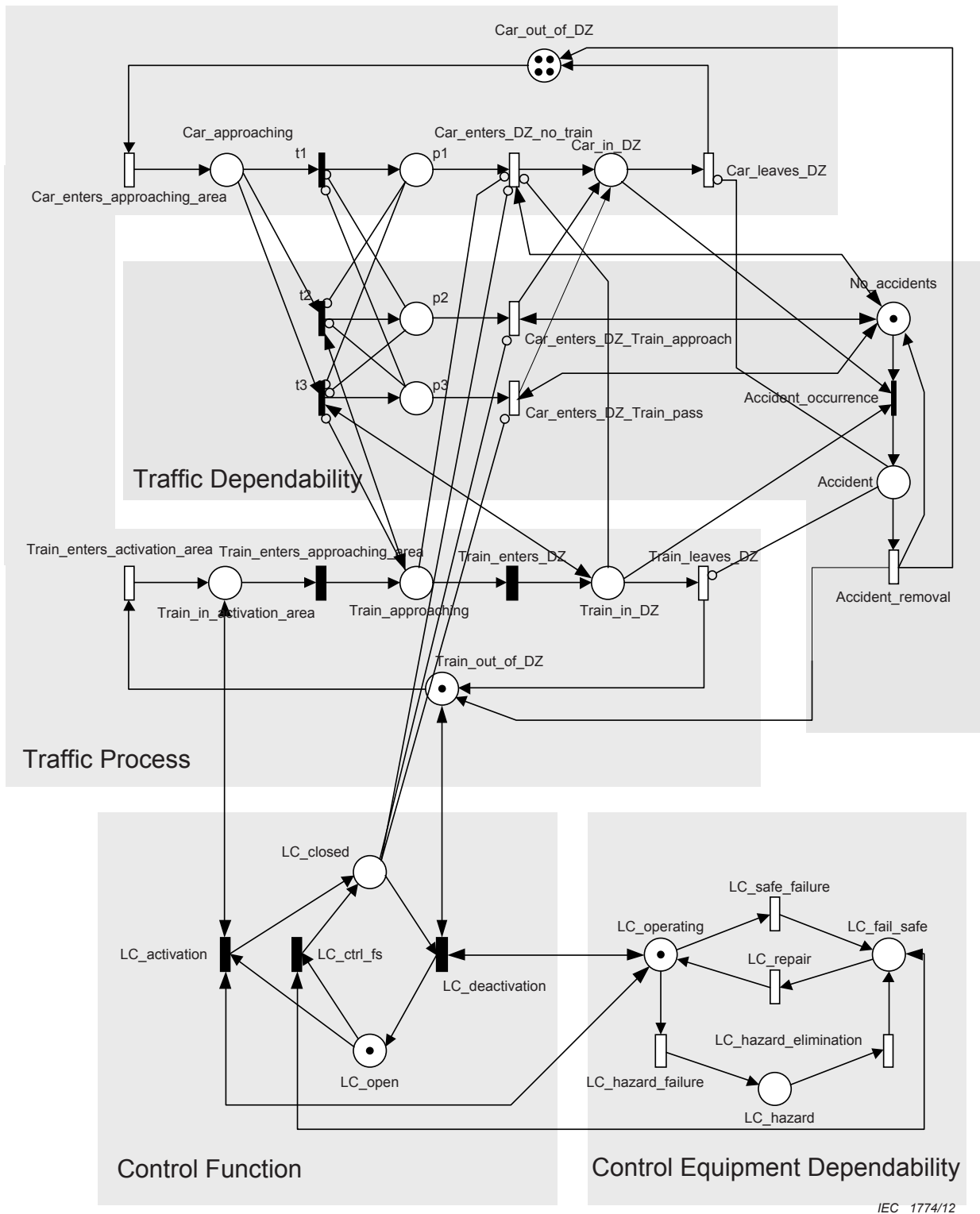


IEC 1773/12

Figure E.6 – PN model of the traffic process with an ideal control function

The existence of an ideal functioning control system leads to the model shown in Figure E.6. In this model, whenever a train is approaching, the level crossing will be activated and closed. Thus, the model in Figure E.6 does not take the dependability parameters of the control function into account; it is assumed that the control function never fails. Consequently, there are no probabilistic transitions in the “control function” submodel, and therefore an accident will never happen.

Finally, the dependability of the control function is taken into account. This means it may fail and therefore accidents may happen, see Figure E.7.



IEC 1774/12

Figure E.7 – PN model of the level crossing example model

E.4.3 Further explanation of the structure and parameters of the model

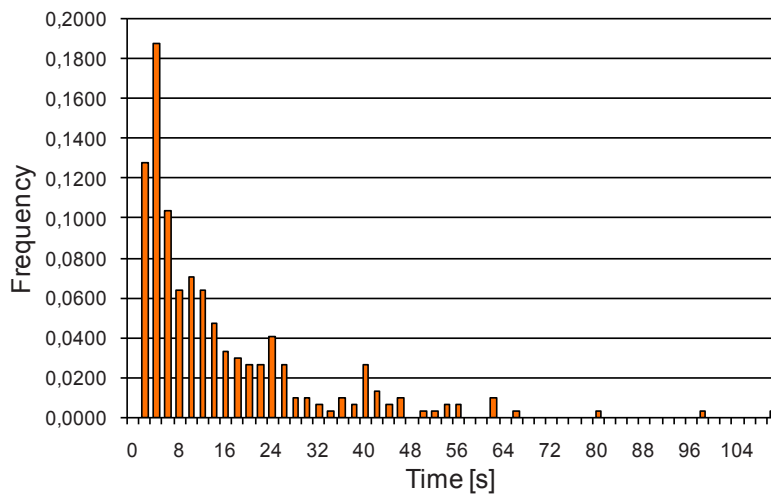
The traffic process submodel describes separately the movement of cars and of trains. Road traffic is represented by six places and eight transitions (the places No_accidents and

Accident as well as the transitions Accident_occurrence and Accident_removal do not directly belong to the traffic process), out of which three are immediate and five are exponential. The places represent the relevant states of the road vehicle as indicated in Table E.1.

Table E.1 – Car-related places in the submodel ‘Traffic process’ (see Figure E.4)

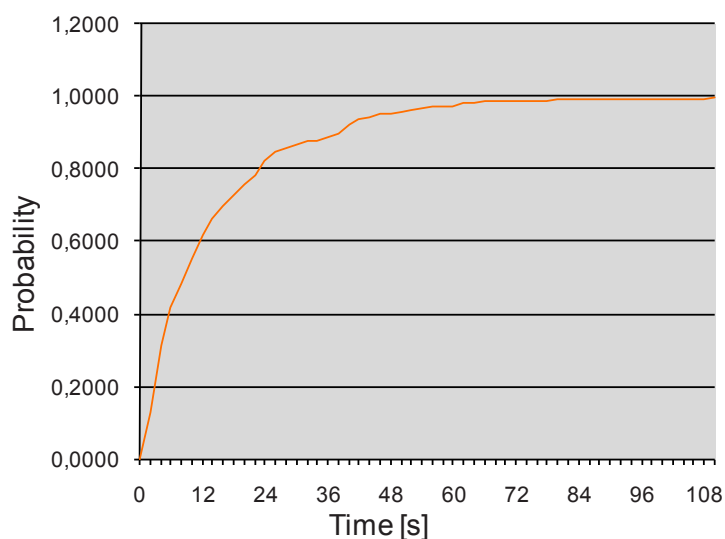
Place	Capacity ^a	Description
Car_out_of_DZ	inf	Car is out of the level crossing system. The multiple tokens are used for representation of a continuous flow of cars
Car_approaching	inf	Car driver approaches the level crossing having the possibility to see the approaching train
<i>p1</i>	1	Car driver approaches the level crossing and is ready to enter the danger zone, as long as there is no train in the vicinity
Car_in_DZ	1	Car is in the danger zone of the LC
NOTE The place ‘Car_approaching’ and ‘ <i>p1</i> ’ are only separated by immediate transitions. Thus, there is no physical difference in the state of the car, the difference lies in the decision of the driver to enter the danger zone or not		
a The “capacity” of a place specifies the maximum number of tokens on that place. A capacity of “inf(imum)” means there are no restrictions concerning the (non-negative) number of tokens on that place.		

The transitions model the dynamics of the car movement. The road traffic flow is described by the transition ‘Car_enters_approaching_area’. The parameter of this transition can be evaluated from the statistical measures of the road traffic flow of a particular level crossing. Figure E.8 shows the measures of the time between two road vehicles in the form of a histogram and Figure E.9 shows the corresponding approximated probability distribution function.



IEC 1775/12

Figure E.8 – Collected measures of the road traffic flow of a particular level crossing: Time intervals between two cars coming to the level crossing

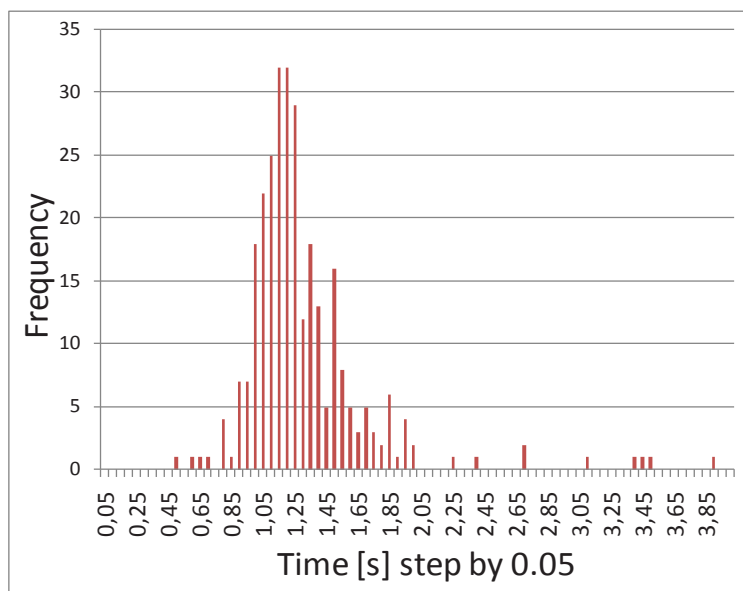


IEC 1776/12

Figure E.9 – Approximated probability distribution function based on the measures depicted in Figure E.5

The presented measures have been approximated by an exponential distribution with an expectancy value of 16,2 s (0,27 min).

In a similar way, the parameter of the transition ‘Car_leaves_DZ’ was evaluated. Figure E.10 reveals the field measures of the particular level crossing.



IEC 1777/12

Figure E.10 – Collected measurements of time spent by road vehicle in the danger zone of the level crossing

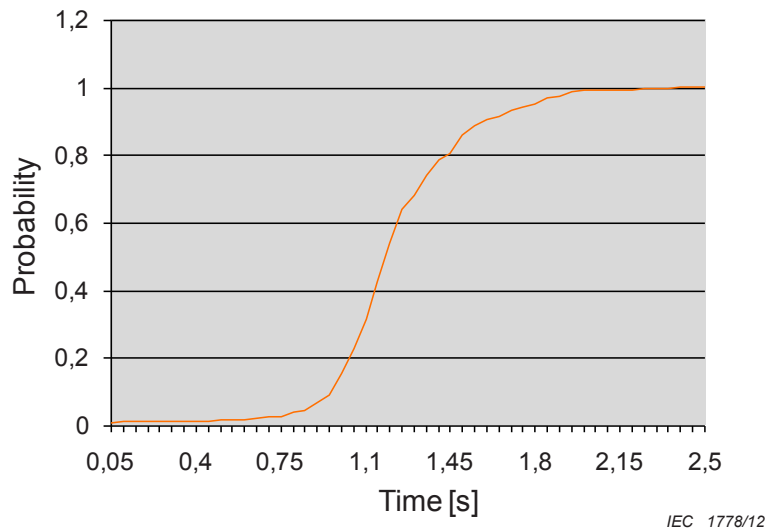


Figure E.11 – Approximated probability distribution function based on measurements depicted in Figure E.10

As can be seen, the corresponding distribution is not exponential. As this parameter has a significant influence on the probability of the accident occurrence, it is recommended to consider the time of the slowest road vehicle as the mean of the exponential distribution function instead of taking just the average time occupancy of the danger zone into account. Therefore, the parameter of the transition 'Car_leaves_DZ' has been set to 3,96 s (0,066 min).

The presented model considers the different possible behaviours of drivers of road vehicles when approaching a level crossing in cases where there is no warning given by the protection equipment (e.g. due to a failure). According to expert estimations, in such a case 50 % of the drivers would enter the danger zone of the level crossing even if they would see an approaching train: firing of transition $t2$ leads to the activation of 'Car_enters_DZ_Train'_approach (presuming that the LC is not closed). With a probability of 45 %, $t1$ fires and marks place $p1$. Transition 'Car_enters_DZ_no_train' is only activated if there is no train in the approaching area or in the danger zone. 5 % of drivers would still enter the danger zone even if a train is passing the level crossing (e.g. due to bad visibility or braking conditions). These considerations are modelled by weighting of immediate transitions $t1$, $t2$ and $t3$ accordingly. The weights are applied when two or more immediate transitions are activated simultaneously. This is for example the case for $t1$ and $t2$ when a car and a train are both in the approaching area (places 'Car_approaching' and 'Train_approaching' are marked).

The parameters of all transitions describing the dynamics of the road traffic (including further explanations) are summarized in Table E.2.

Table E.2 – Car-traffic related transitions in the submodel ‘Traffic process’ and Traffic dependability (see Figure E.7)

Transition name	Time concept	Weight parameter	Time min	Description
Car_enters_approaching_area	Exponentially distributed	–	0,27	Describes the road traffic flow (see above)
r_1	Immediate	95	–	Describes the case of a road vehicle entering the danger zone only if there is no train
r_2	Immediate	95	–	Describes the case of a road vehicle entering the danger zone if a train is approaching and no warning is given
r_3	Immediate	5	–	Describes the case of a road vehicle entering the danger zone if a train is passing and no warning is given
Car_enters_DZ_no_train	Exponentially distributed		0,1	Describes the time a car spends in the approaching area
Car_enters_DZ_Train_approach	Exponentially distributed		0,1	Describes the time a car spends in the approaching area
Car_enters_DZ_Train_pass	Exponentially distributed		0,1	Describes the time a car spends in the approaching area
Car_leaves_DZ	Exponentially distributed		0,066	Describes the time a car spends in the danger zone

The parameters of all places describing the dynamics of the road traffic (including further explanations) are summarized in Table E.3.

Table E.3 – Train-traffic related places in the submodel ‘Traffic process’ (see Figure E.7)

Place name	Capacity	Description
Train_out_of_DZ	1	Train is outside of the level crossing system
Train_in_activation_area	1	Train is in the area in which the level crossing protection equipment (warning lights) is activated and the visual warning starts
Train_approaching	1	Train is in the area in which it is visible to a car driver in the approaching area
Train_in_DZ	1	Train is in the danger zone of the LC

The dynamics of the rail traffic is described by the transitions. The flow of the railway traffic is described by the transition ‘Train_enters_activation_area’, whose parameter is evaluated based on the analysis of the time table. The average frequency of trains in the given example is two trains per hour, assuming exponential distribution of the times between two trains. The example further assumes the same speed of all trains leading to constant times that the head of the train is spending in the activation and approaching area of the level crossing ($T_{AC} = \text{const.} = 0,133 \text{ min} + 0,166 \text{ min}$). The time spent in the danger zone depends on the length of the train. Its variation is assumed according to the exponential distribution with the mean time of 0,3 min.

The rail traffic transition’s distributions and parameter meanings are summarized in Table E.4.

Table E.4 – Train-traffic related transitions in the submodel ‘Traffic process’ (see Figure E.7)

Transition name	Time concept	Time min	Description
Train_enters_activation_area	Exponentially distributed	30	Describes the flow of the rail traffic
Train_enters_approaching_area	Deterministic	0,133	Describes the time the train spends in the activation area (activates warning).
Train_enters_DZ	Deterministic	0,166	Describes the time the train spends in the approaching area (visible for car driver).
Train_leaves_DZ	Exponentially distributed	0,5	Describes the time the train spends in the danger zone

The interaction between the road and rail traffic processes is represented by test and inhibitor arcs. These are especially used when modelling the decision of the car driver to enter into the danger zone and the interaction between the cars (immediate transitions $t1$, $t2$ and $t3$ can be activated only if there is no car ready to enter the danger zone on places $p1$, $p2$ and $p3$).

The possibility of an accident is modelled in the submodel ‘Traffic dependability’. The occurrence is modelled by two arcs from places ‘Car_in_DZ’ and ‘Train_in_DZ’ of the ‘Traffic Process’ subnet. There is no temporality assumed, all the accidents are considered immediate logical consequences of the contemporaneous presence of the road and rail vehicle in the danger zone of the level crossing. The accident removal procedure is assumed to have an exponentially distributed duration of 2 h (120 min) on average. During the accident removal, the level crossing is not available for rail and for road traffic (modelled by corresponding inhibitors). The meaning of the places and transition as well as their parameters is summarized in Tables E.5 and E.6.

Table E.5 – Places in the submodel ‘Traffic dependability’ (see Figure E.7)

Place name	Capacity	Description
No_Accidents	1	No accidents in the danger zone
Accident	1	Accident in the danger zone
$p2$	1	Car driver approaches the level crossing and is ready to enter the danger zone, even if there is a train approaching (as long as the warning device is not on)
$p3$	1	Car driver approaches the level crossing and is ready to enter the danger zone, even if there is a train passing through (as long as the warning device is not on)

Table E.6 – Transitions in the submodel ‘Traffic dependability’ (see Figure E.7)

Transition name	Time concept	Weight	Time min	Description
Accident_occurrence	Immediate	1		Describes logical consequences of contemporaneous occupancy of the danger zone by car and train
Accident_removal	Exponentially distributed	–	120	Describes duration of the procedure of the accident removal

The subnet ‘Control function’ describes the influence of the level crossing protection equipment on the traffic processes. The places ‘LC_open’ and ‘LC_closed’ represent the main system states of the equipment. The activation of the equipment (transition “LC_activation”) is modelled by the test arc connected with the place of the traffic process model, representing

the train in the activation area. A further cause of activation is the detection of a failure of the equipment modelled as a safe failure state in the ‘Control equipment dependability’ subnet (e.g. failure of the wheel detector for deactivation of the protection equipment or any kind of other detected failures). The deactivation of the equipment (‘LC_deactivation’) takes place the moment when the train has left the danger zone (test-arc connection with the place ‘Train_out_of_DZ’), as long as the equipment is in the operating state. The model assumes that if the level crossing protection equipment is in the warning state, no car driver decides to enter the danger zone (modelled by inhibitors towards the transitions in traffic processes subnet). Further extensions of the model can also be used to model a more realistic behaviour of the car drivers, in terms of ignoring the warning lights. Tables E.7 and E.8 summarize the meaning and parameters of the places and transitions belonging to the ‘Control function’ submodel.

Table E.7 – Places in the submodel ‘Control function’ (see Figure E.7)

Place name	Capacity	Description
LC_open	1	LC is in its passive state, the warning for road user is off
LC_closed	1	LC is in its active state, the warning for road user is on

Table E.8 – Transitions in the submodel ‘Control function’ (see Figure E.7)

Transition name	Time concept	Weight parameter	Description
LC_activation	Immediate	1	Describes the activation of the LC protection equipment
LC_deactivation	Immediate	1	Describes the deactivation of the LC protection equipment
LC_ctrl_fs	Immediate	1	Describes the activation of the LC due to the detection of a failure of the protection equipment

The internal dependability states of the level crossing protection equipment are modelled in the subnet “Control equipment dependability”. It consists of the three relevant states representing the operating, fail-safe and hazard state. The exponential transitions model the possible state changes (similar to using a Markov chain). Using test arcs in Figure E.3 to connect the subnets of the control function equipment models the influence of the dependability states on the functionality of the level crossing protection equipment. In particular, it can be seen that if the protection equipment is in a hazard state (e.g. failure of the train detection device or any kind of undetected failure of the protection equipment) no activation of the warning of road vehicle drivers is possible.

Tables E.9 and E.10 summarize the meaning and parameters of the places and transitions belonging to the ‘Control equipment dependability’ submodel.

Table E.9 – Places in the submodel ‘Control equipment dependability’ (see Figure E.7)

Place name	Capacity	Description
LC_operating	1	LC is in operating state, the LC protection equipment functionality (activation and deactivation) is fully available
LC_fail_safe	1	LC is in safe failure state, the LC protection equipment is in a safe state – the warning for road user is on
LC_hazard	1	LC is in a hazard state, the LC protection equipment functionality (activation and deactivation) is not available

**Table E.10 – Transitions in the submodel ‘Control equipment dependability’
(see Figure E.7)**

Transition name	Time concept	Time min	Description
LC_hazard_failure	Exponentially distributed	6×10^6	Describes the time to occurrence of the hazard failure of the LC protection equipment
LC_safe_failure	Exponentially distributed	6×10^5	Describes the time to occurrence of the safe failure of the LC protection equipment
LC_hazard_elimination	Exponentially distributed	360	Describes the time to detection of a hazard failure of the LC protection equipment
LC_repair	Exponentially distributed	240	Describes the time to repair of the LC protection equipment (after a detected failure)

The temporal parameter of the transition ‘LC_hazard_failure’ is the mean time to a hazardous failure and corresponds to the safety integrity level of the level crossing protection equipment. The model assumes that the occurrence rate of the safe system failure is ten times higher than the hazard rate occurrence. The parameter of the transition ‘LC_hazard_elimination’ can be obtained by analysis of statistical data or taking the longest delay between two trains (assuming e. g. the detection of a hazard failure of the LC protection equipment by the train driver) which was 6 h (360 min), into account. The temporal parameter of the transition ‘LC_repair’ is estimated to be 4 h (240 min) which represents the repair time after a failure detection, including activation, travel and repair time of the maintenance crew.

There are no specific transition guards defined; this means that all guards can be seen as ‘true’ or ‘fulfilled’. The preemption policy is ‘preemption repeat different’ for all the transitions.

E.5 Analysing the model to achieve results of interest

In the fourth step the model is analysed to achieve the results of interest and the analyses are documented (see 5.2.5).

The task of qualitative analysis is to investigate the state space of the model. The qualitative reachability graph of the net is generated. The corresponding graph has 300 states. It is not possible to visualize such a graph; instead an aggregated graph has been constructed.

The task of the quantitative analysis is to evaluate the occurrence rate of accidents in dependence on the parameters of transitions used in the model (e.g. number of trains or road vehicles per hour, length of used activation time T_{AC} , safety integrity level (SIL, see EN 50126 [21]) of the protection equipment, etc.). As there are exponentially distributed as well as determined timed transitions and causal transitions, Monte Carlo simulations led to the analysis results.

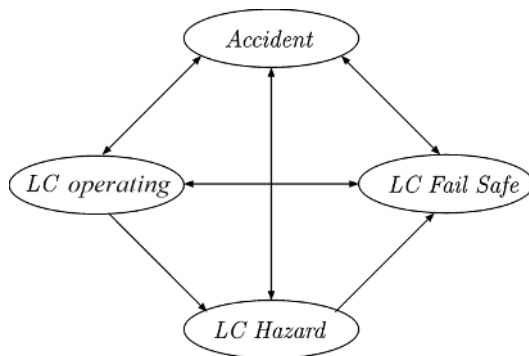
All the analyses have been performed with the PN-Tool TimeNet in version 4.0 (see [22]) and have been confirmed by the use of the tool π -Tool [23].

The calculation was performed on an ‘Asus P4B533’-board, Intel Pentium 4 CPU 2,4 GHz with 1 024 MB RAM. As the model takes the ‘accident removal’ into account, only one history had to be simulated. The history duration was about 250 million years and the computing time about 120 days. This could be shortened to a few days through a mathematical pre-process without any influence on the simulation result.

E.6 Representation and interpretation of results

In the fifth step, the results of the analyses are represented and interpreted and this representation is documented (see 5.2.6).

Concerning qualitative analysis, using the visualization by the aggregated reachability graph, some obvious relations between the main global states can be checked. As an example, the aggregated RG in Figure E.12 reveals the occurrence of major dependability states of the level crossing protection equipment and their relation to the accident state. As can be seen, the graph confirms the modelled sequence of the dependability states (operating, hazard, fail-safe), and shows that an accident can occur independently from the dependability state of the level crossing protection equipment (in any case, the situation that a car entered the danger zone and stayed there until a train arrived can occur), as shown in Figure E.12.



IEC 1779/12

Figure E.12 – Aggregated RG and information about the corresponding states

In Table E.11 the number of states of the PN model subsumed in the corresponding aggregated state (due to the Boolean condition) is indicated.

Table E.11 – Specification of boolean conditions for states to be subsumed in an aggregated state

Name of aggregated state	Boolean condition	Number of states of the (ordinary) RG that are subsumed in the state of the aggregated RG
Accident	$m(\text{accident}) \geq 1$	39
LC operating	$m(\text{LC_operating}) \geq 1 \wedge m(\text{accident}) = 0$	71
LC Hazard	$m(\text{LC_hazard}) \geq 1$ $\wedge m(\text{accident}) = 0$	100
LC Fail Safe	$m(\text{LC_fail_safe}) \geq 1 \wedge m(\text{accident}) = 0$	90

NOTE ‘ \wedge ’ specifies the logical ‘and’; $m(\text{place})$ denotes the marking of a place, i.e. the number of tokens on that place.

The results of the quantitative analysis can be used on the one hand to evaluate the availability of the level crossing for the road traffic. It is expected that the availability will increase by shortening the activation time T_{AC} of the level crossing warning (before arrival of the train), and also with a decrease of the hazard failure occurrence rate (especially because of the assumption that in this case also the occurrence rate of the fail safe failure is linearly (1:10) increased). Figure E.13 confirms these expectations.

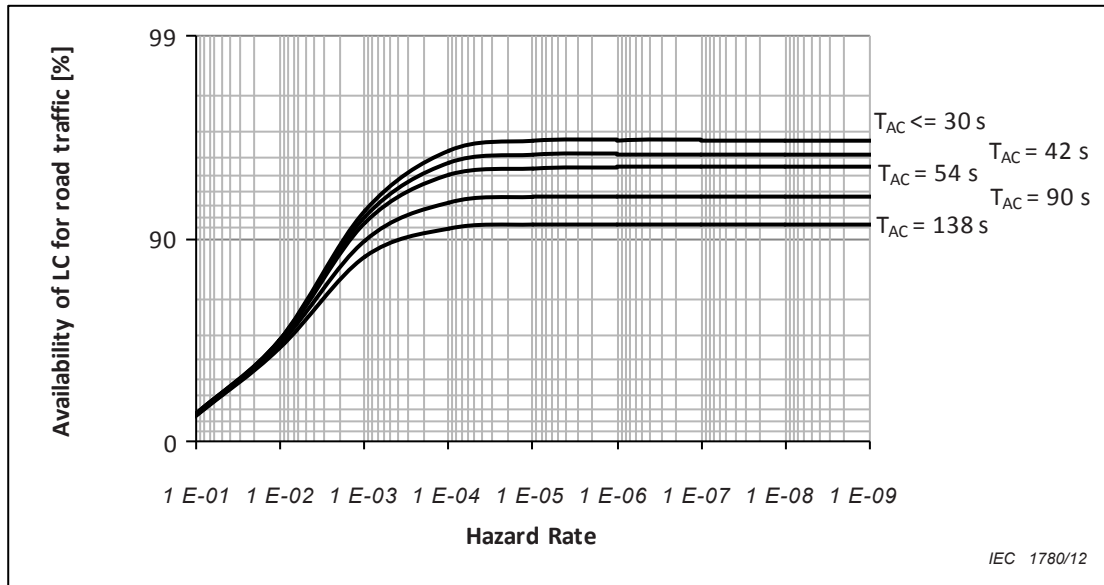


Figure E.13 – Results of the quantitative analysis showing the level crossing average availability for road traffic users as a function of the protection equipment hazard rate for different used activation and approaching times T_{AC}

On the other hand, the results of the quantitative analysis can be used to evaluate the road traffic safety. Considering the given flow of the road vehicles and the average occupancy of a car by 1,5 persons and fatality factor 1, the obtained occurrence rate of accidents can be used to evaluate the individual risk of the road users at the level crossing (road users' mortality in the form of fatalities per person and year). Figure E.14 reveals the dependence of the individual road user risk from the used activation time T_{AC} and the hazard rate of the level crossing protection equipment.

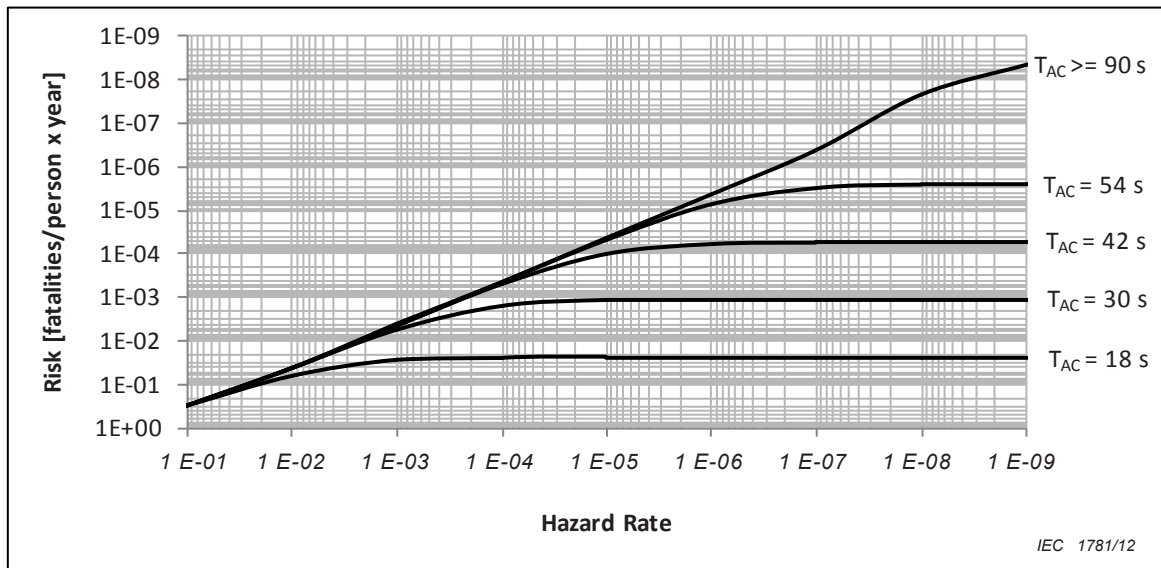


Figure E.14 – Results of the quantitative analysis showing the individual risk of the level crossing users as a function of the protection equipment hazard rate for different used activation and approaching times T_{AC}

As can be seen in Figures E.13 and E.14, some technical improvements leading to the increase of the safety integrity level (decrease of the hazard rate) are unnecessary and may only lead to an increase of system development and production costs. The visualization of the

quantitative analysis results by the safety/availability diagram given in Figure E.15 reveals an appropriate possibility for optimization prospects.

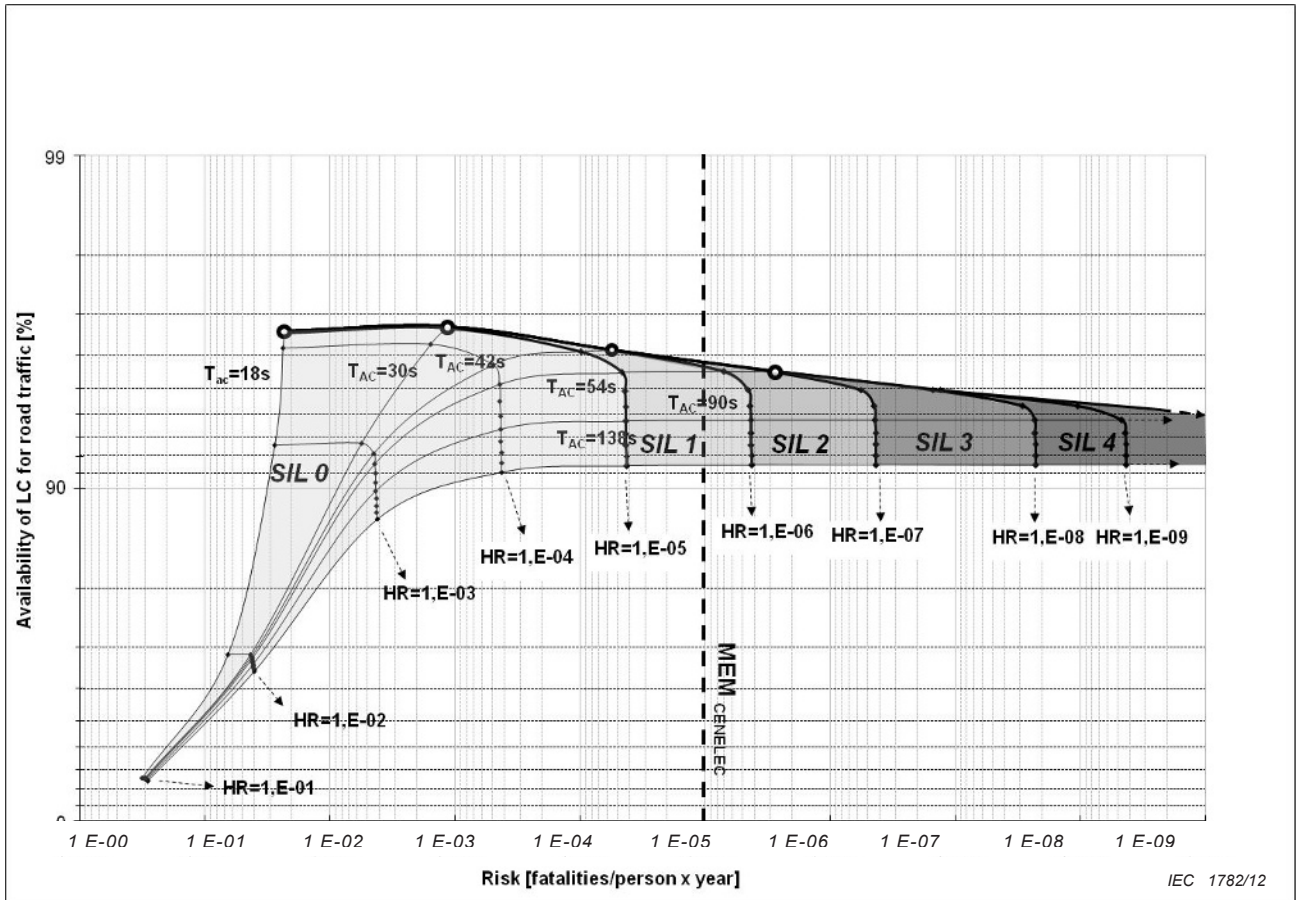


Figure E.15 – Availability safety diagram based on the quantitative results of the model analysis shown in Figure E.13 and Figure E.14

Figure E.15 reveals that the optimal value of the activation time T_{AC} is at about 54 s, allowing to decrease the risk that the road vehicle might not able to clear the danger zone satisfactorily. This value reveals the possibility of using the technology of the safety integrity level 1 ($HR = 1 E-5 - 1 E-6$), providing an availability rate of the level crossing for the road traffic of 94,5 %, and the individual risk of 1 E-5 fatalities per person and per year (the risk acceptance value $MEM_{CENELEC}$ is the “Minimal endogenous mortality” given by EN 50126 [21]).

Bibliography

Cited references in order of appearance

- [1] PETRI, C.A., *Kommunikation mit Automaten*. Schriften des Instituts für instrumentelle Mathematik, Bonn, 1962
- [2] IEC 61508 (all parts), *Functional safety of electrical/electronic/ programmable electronic safety-related systems*
- [3] GERMAN, R., *Performance Analysis of Communication Systems – Modelling with Non-Markovian Stochastic Petri Nets*, John Chichester: Wiley, 2000
- [4] MURATA, T., *Petri nets: Properties, Analysis and Application*. In: Proceedings of the IEEE, Vol. 77, pages 541-580, 1989
- [5] IEC 60050-151:2001, *International Electrotechnical Vocabulary – Part 151: Electrical and magnetic devices*
- [6] IEC 60050-111:1996, *International Electrotechnical Vocabulary – Part 111: Physics and chemistry*
Amendment 1 (2005)
- [7] IEC 60050-351:2006, *International Electrotechnical Vocabulary – Part 351: Control technology*
- [8] IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations²*
- [9] IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*
- [10] ISO/IEC 15909-1, *Software and system engineering – High-level Petri nets – Part 1: Concepts, definitions and graphical notation*
- [11] MALHOTRA, M., TRIVEDI K.S., *Dependability Modelling Using Petri Nets*, IEEE Transactions on Reliability Vol 44, no 3
- [12] SIGNORET, J.-P., *Modelling the behaviour of complex industrial systems with stochastic Petri nets*. Proc., European Safety and Reliability Conference (ESREL), Trondheim, Norway, 16-19 June
- [13] Petri Nets World – Tools and Software: URL: <http://www.informatik.uni-hamburg.de/TGI/PetriNets/tools/>
- [14] JENSEN, K., *Coloured Petri Nets: Basic concepts, Analysis Methods and Practical Use*, Volume 1 – 3, Springer, New York 1997
- [15] CODETTA-RAITERI, D., *Extended Fault Trees Analysis supported by Stochastic Petri Nets*, Ph. D. thesis, Università degli Studi di Torino, 2005
- [16] BAUSE, F., KRITZINGER P.S., *Stochastic Petri Nets, An Introduction to the Theory*, 2nd Edition, Vieweg, Braunschweig/Wiesbaden, 2002
- [17] MOLLOY, M.K., *Performance analysis using stochastic Petri nets*, In IEEE Transaction on Computer Sciences, 1982
- [18] TRIVEDI, K.S., *Probability and Statistics with Reliability, Queuing, and Computer Science Applications*, Wiley & Sons, 2nd ed., 2001
- [19] IEC 61165:2006, *Application of Markov techniques*

² The cited term, “module” (definition 3.3) does not appear in the latest edition.

- [20] *Resilience-Building Technologies: State of Knowledge*. ReSIST project deliverable D12, URL: <http://www.resist-noe.org/Publications/Deliverables/D12-StateKnowledge.pdf>
- [21] EN 50126: 2001, *Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*
- [22] ZIMMERMANN, A. et al.: "*Timenet 3.0 tool description*," in *Int. Conf. on Petri Nets and Performance Models (PNPM 99), Tool descriptions*. Zaragoza, Spain: University of Zaragoza, 1999
- [23] *π -Tool: Tool for modelling and analysis with stochastic Petri nets* developed at the Institute for Traffic Safety and Automation Engineering of the Technical University of Braunschweig

Uncited references

- IEC 60812:2006, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*
- IEC 61025:2006, *Fault tree analysis (FTA)*
- IEC 61078:2006, *Analysis techniques for dependability – Reliability block diagram and boolean methods*
- IEC 61511-3:2003, *Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels*
- IEC 61703:2001, *Mathematical expressions for reliability, availability, maintainability and maintenance support terms*
- BAUMGARTNER, B., *Petri-Netze; Grundlagen und Anwendungen, 2. Auflage*. Spektrum – Akademischer Verlag, Heidelberg, 1996
- NICOL, D.M., SANDERS, W.H., TRIVEDI, K.S., *Model-based Evaluation: From Dependability to Security*. IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 1, pp 48-65, 2004
- DUTUIT, Y., et al., *Dependability modelling and evaluation by using stochastic Petri nets: application to two test cases*, Reliability Engineering and System Safety, vol. 55, n°2, 1997, pp.117-124
- MARSAN, M. A., et al.: *Modelling with generalized stochastic Petri Nets*. Wiley Series in Parallel Computing, John Wiley & Son Ltd, 1996.
- CHABOT, J., DUTUIT, Y. RAUZY, A., SIGNORET, J.P., *An engineering approach to optimize system design or spare parts inventory*, Risk decision and Policy, vol. 8, 2003, pp. 1-11
- SIGNORET, J.P., DUTUIT, Y., *Tutorial on dynamic system modelling by using stochastic Petri nets and Monte Carlo simulation*, Konbin'03 International Conference, Gdansk, Poland 2003
- GIRAULT, C., VALK, R., *Petri Nets for Systems Engineering*. Springer 2003
- SCHNEEWEISS, W.G., *Petri Nets for Reliability Modelling*. LiLoLe 1999
- SCHNEEWEISS, W.G., *Petri Net Picture Book*. LiLoLe 2004
-

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services. It presents the UK view on standards in Europe and at the international level.

BSI is incorporated by Royal Charter. British Standards and other standardisation products are published by BSI Standards Limited.

Revisions

British Standards and PASs are periodically updated by amendment or revision. Users of British Standards and PASs 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 British Standards would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Similar for PASs, please notify BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers BSI Subscribing Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of British Standards and PASs.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001

Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website www.bsigroup.com/shop. In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

Email: orders@bsigroup.com

In response to orders for international standards, BSI will supply the British Standard implementation of the relevant international standard, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005

Email: knowledgecentre@bsigroup.com

BSI Subscribing Members 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: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001

Email: membership@bsigroup.com

Information regarding online access to British Standards and PASs via British Standards Online can be found at www.bsigroup.com/BSOL

Further information about British Standards is available on the BSI website at www.bsi-group.com/standards

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that own copyright in the information used (such as the international standardisation bodies) has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. This does not preclude the free use, in the course of implementing the standard, of necessary details such as symbols, and size, type or grade designations. If these details are to be used for any other purpose than implementation then the prior written permission of BSI must be obtained. Details and advice can be obtained from the Copyright & Licensing Department.

Tel: +44 (0)20 8996 7070

Email: copyright@bsigroup.com

BSI

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001

Fax +44 (0)20 8996 7001

www.bsigroup.com/standards