IEC 62551

Edition 1.0 2012-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Analysis techniques for dependability – Petri net techniques

Techniques d'analyse de sûreté de fonctionnement – Techniques des réseaux de Petri

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,…).
It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,…).
Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications de la CEI. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

IEC 62551

Edition 1.0 2012-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Analysis techniques for dependability – Petri net techniques

Techniques d'analyse de sûreté de fonctionnement – Techniques des réseaux de Petri

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX XB

ICS 21.020

ISBN 978-2-83220-370-5

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

ANALYSIS TECHNIQUES FOR DEPENDABILITY – PETRI NET TECHNIQUES

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62551 has been prepared by committee 56: Dependability.

The text of this standard is based on the following documents:

FDIS	Report on voting
56/1476/FDIS	56/1484/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

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 combinatory 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

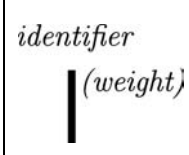
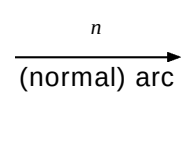
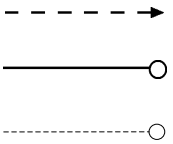
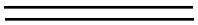
						
Place symbol, also used for multiple places	Transition symbol	Transition symbol with a transition weight	Relation symbols – normal arcs	Relation symbols – test arcs	Relation symbols – inhibitor arcs	Token symbol
There are various possibilities to draw test- and inhibitor-arcs. The token symbol is not 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	$\varnothing$ 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

Identifier 	*Identifier* 	*Identifier* 	
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.

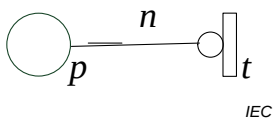


Figure 1 – Weighted inhibitor arc

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.

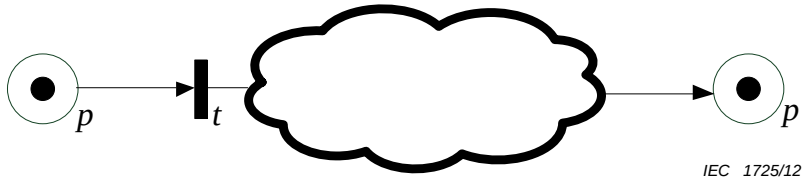


Figure 2 – Place *p* is a multiple place

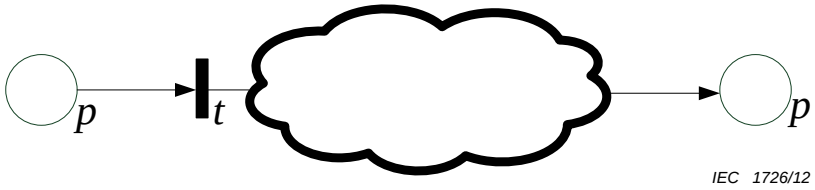


Figure 3 – Marking on *p* after firing of transition *t*

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.

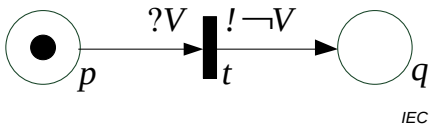


Figure 4 – The activation of *t* depends on the value of *V*

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. $!\neg V$ sets the value of the global variable V to false: $\neg V$ 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).

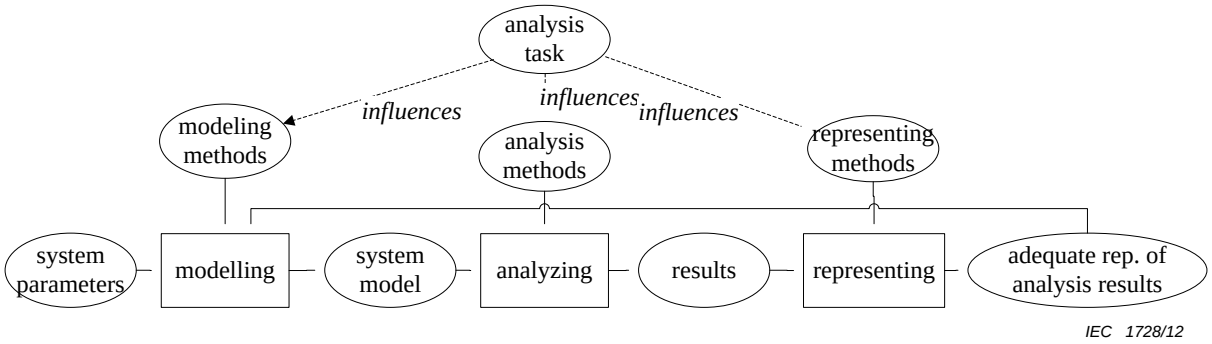


Figure 5 – Methodology consisting mainly of 'modelling', 'analysing' and 'representing' steps

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.

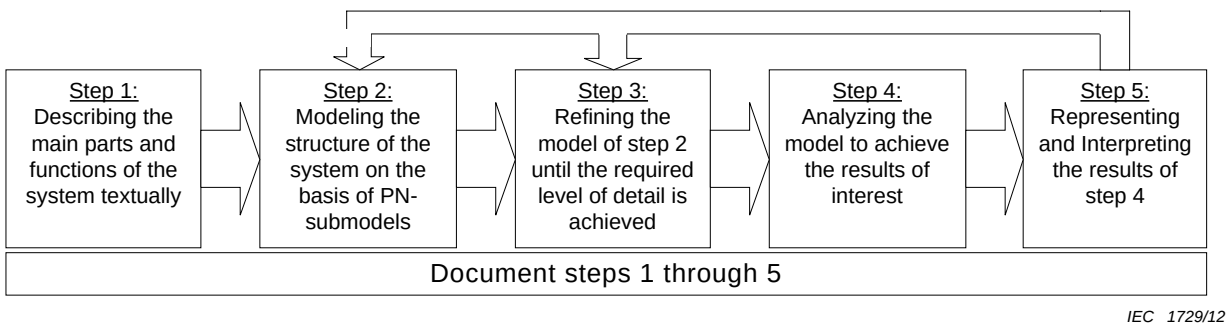


Figure 6 – Process for dependability modelling and analysing with Petri nets

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.

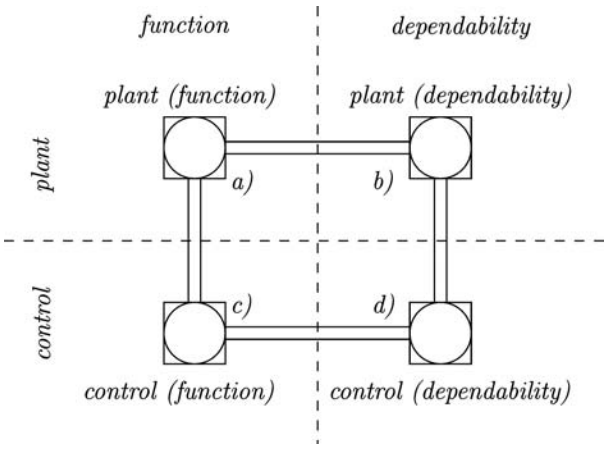


Figure 7 – Modelling structure concerning the two main parts 'plant' and 'control' with models for their functions and dependability

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.

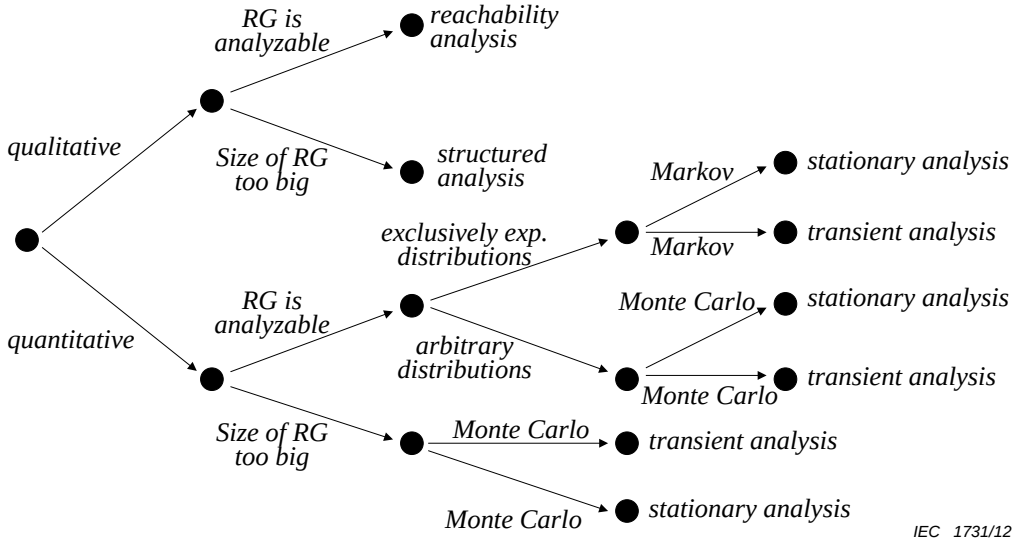


Figure 8 – Indication of the analysis method as a function of the PN model

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 '$comp_1$ faulty' is an abbreviation for '$component_1$ 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.

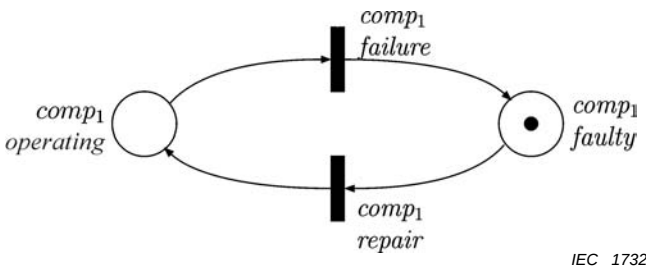


Figure A.1 – Availability state-transition circle of a component

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.

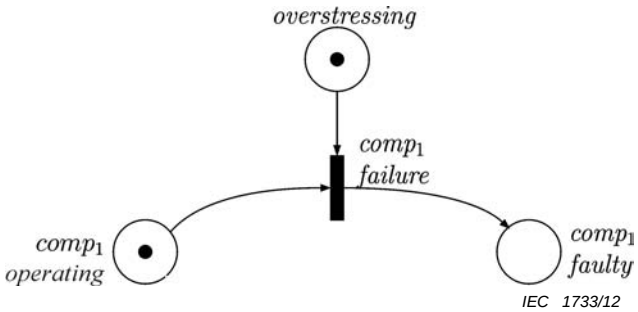


Figure A.2 – Transition 'failure' is enabled

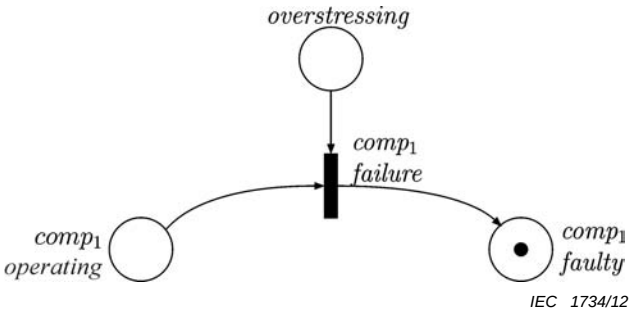


Figure A.3 – 'Faulty' place marked due to firing of 'failure'

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.

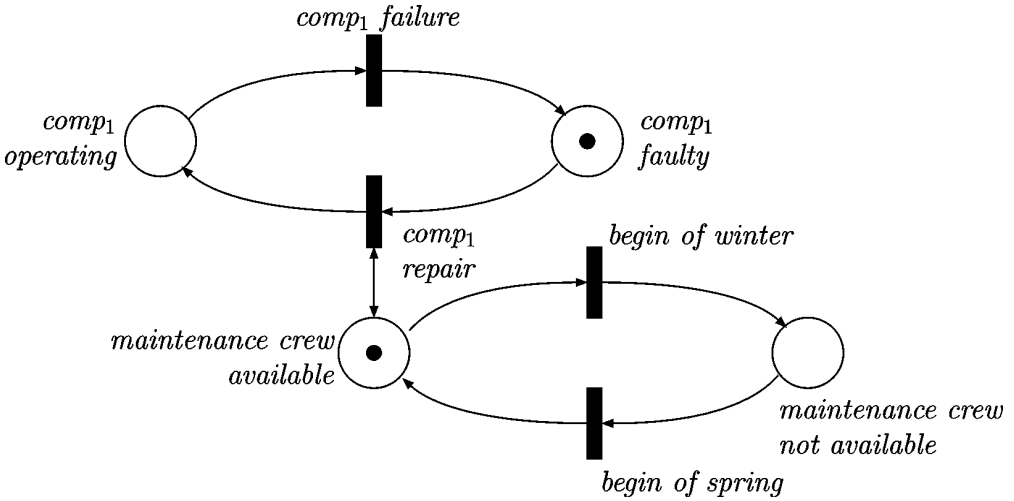


Figure A.4 – Transition 'comp$_1$ repair' is enabled

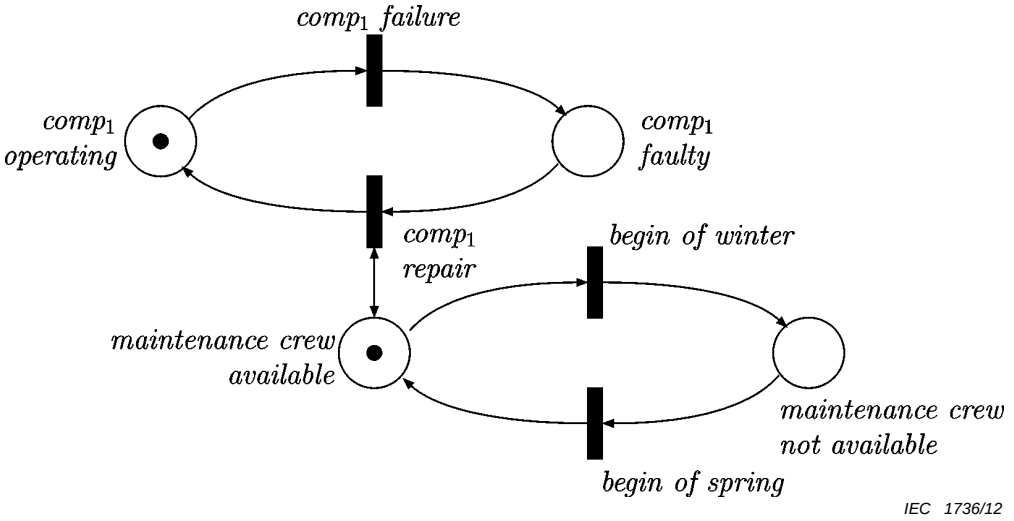


Figure A.5 – The token at the 'maintenance crew available' location is not used

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.

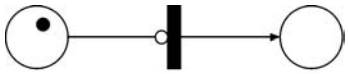


Figure A.6 – Transition is not enabled

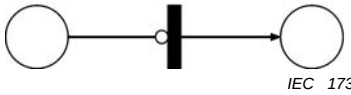


Figure A.7 – Marking before firing

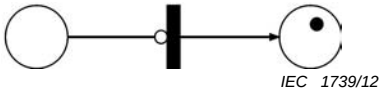


Figure A.8 – Marking after firing

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.

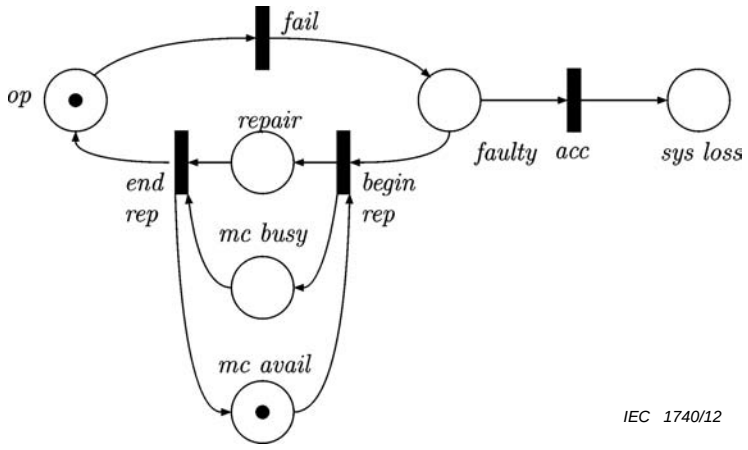


Figure A.9 – PN with initial marking

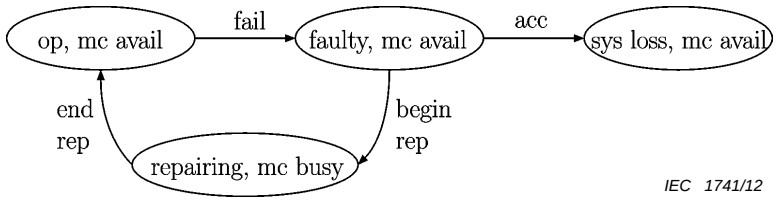


Figure A.10 – Corresponding RG

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 '$comp_{low\text{-}priority}$ faulty' is marked, maintenance crews are available (at least one crew is needed to repair this component) and the '$comp_{high\text{-}priority}$' is not faulty. In addition, transition '$comp_{hp}$ failure' (abbrev. for '$component_{high\ priority}$ failure') is enabled due to the fulfilment of condition '$comp_{high\text{-}priority}$ operating'.

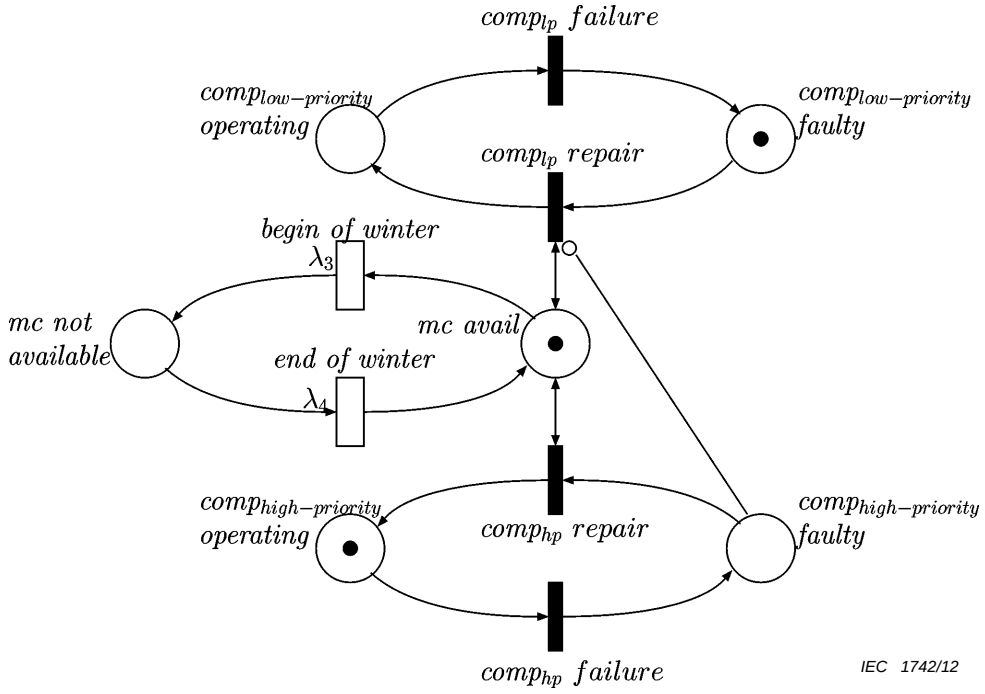


Figure A.11 – Transitions '$comp_{lp}$ repair' and '$comp_{hp}$ failure' are enabled

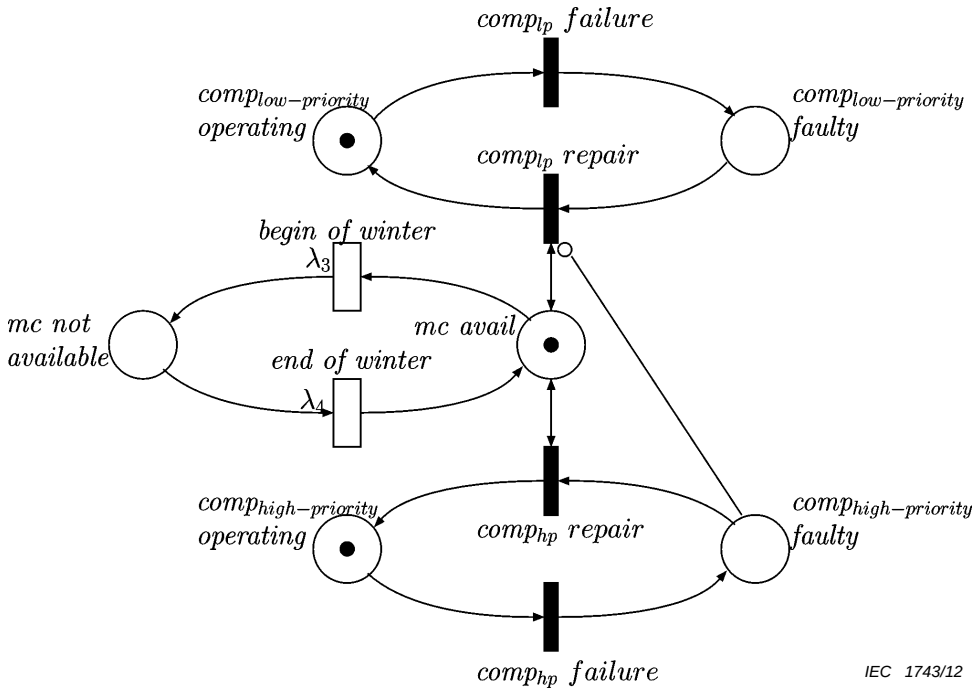


Figure A.12 – Marking after firing of transition '$comp_{lp}$ repair'

Firing of '$comp_{lp}$ repair' absorbs one token from place '$comp_{low\text{-}priority}$ faulty' and produces one token on place '$comp_{low\text{-}priority}$ operating'. As places '$comp_{high\text{-}priority}$ faulty' and 'maintenance-crew available' are connected with transition '$comp_{lp}$ 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

a) the repair of the low priority component is suspended,

b) the repair of the high priority component starts,

c) 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.

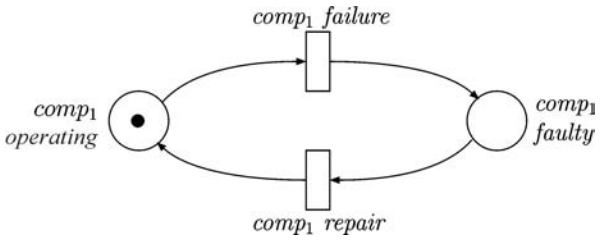


Figure A.13 – A timed PN with two exponentially distributed timed transitions

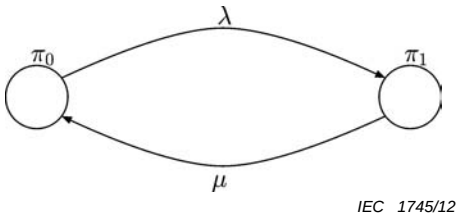


Figure A.14 – The corresponding stochastic reachability graph

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

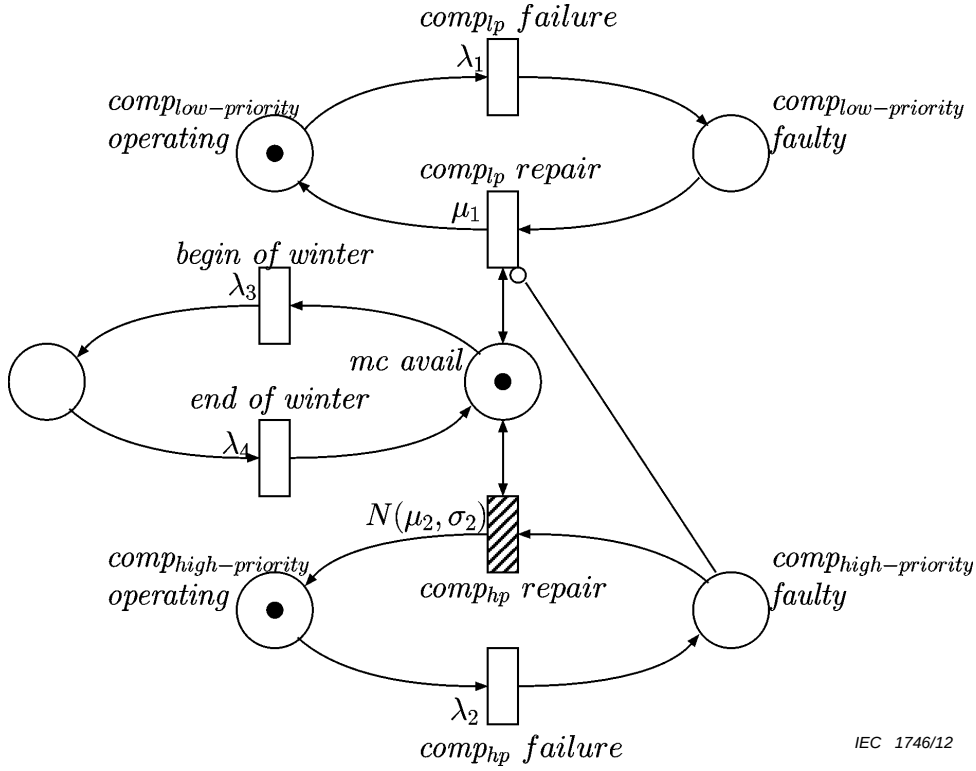


Figure A.15 – Petri net with timed transitions

In Figure A.15 the transition 'comp$_{lp}$ failure' fires with rate λ_1, i.e. once this component is in its operating state (denoted as comp$_{low\text{-}priority}$ 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,∞) 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 PNs (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 age are given in Table A.2.

Table A.2 – Place and transition with rewards

Identifier *rr* 	Identifier *ir* 
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.

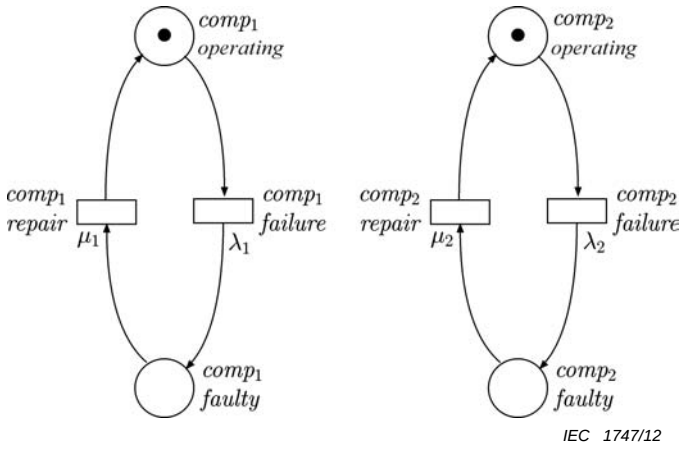


Figure B.1 – Two individual item availability nets with specific failure- and repair-rates

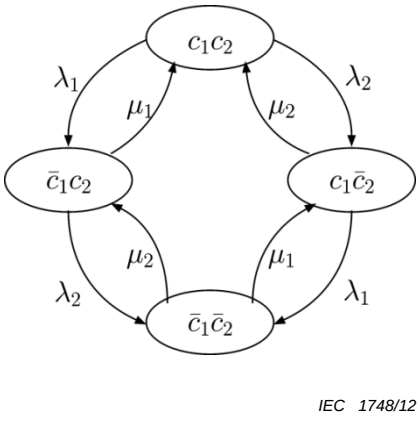


Figure B.2 – Stochastic reachability graph corresponding to Figure B.1 with global states (as an abbreviation $\bar{c}_1$ is used for "*comp*$_1$ faulty")

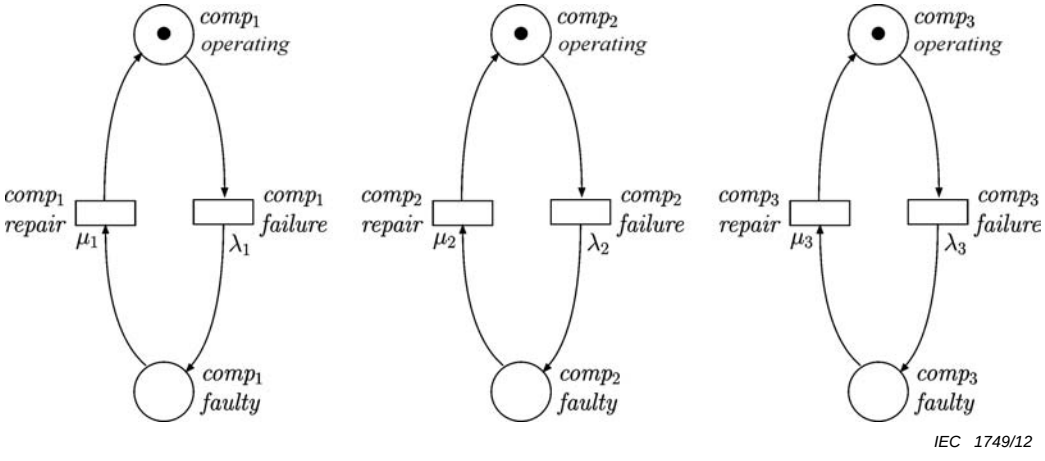


Figure B.3 – Three individual item availability nets with specific failure rates and repair rates

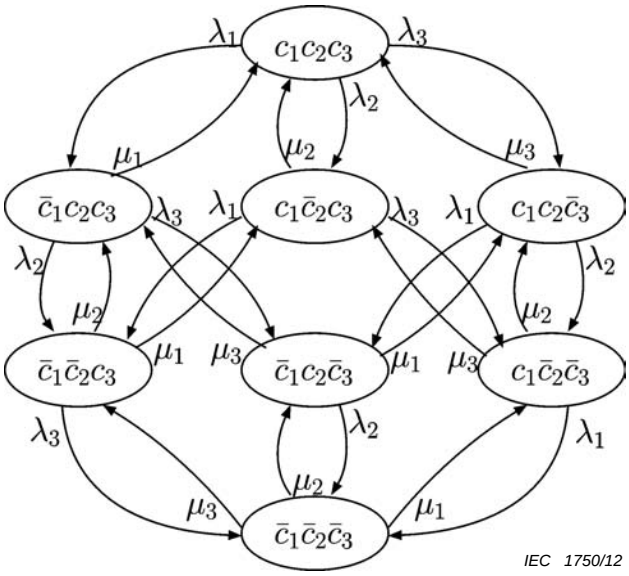


Figure B.4 – Stochastic reachability graph corresponding to Figure B.3 with global states (as an abbreviation $\bar{c}_1$ is used for 'comp$_1$ faulty')

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.

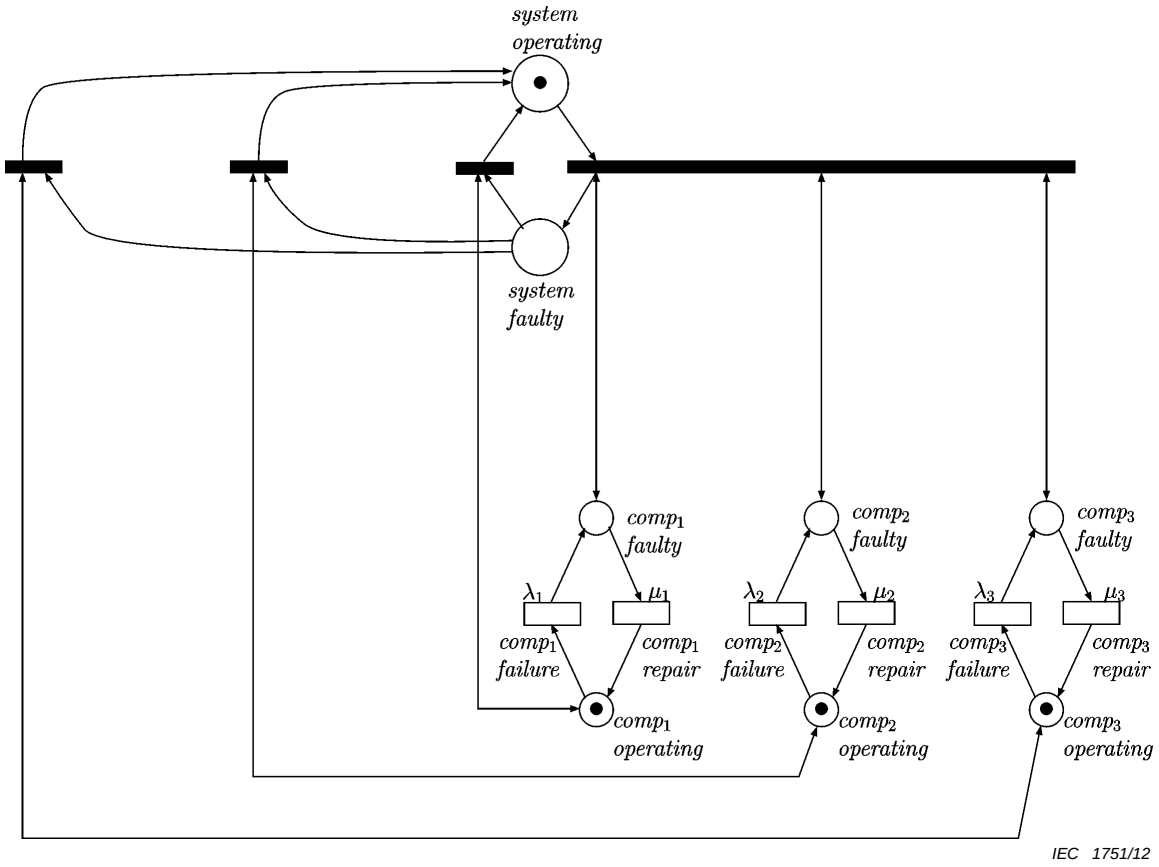


Figure B.5 – Specifically connected 1-out-of-3 availability net

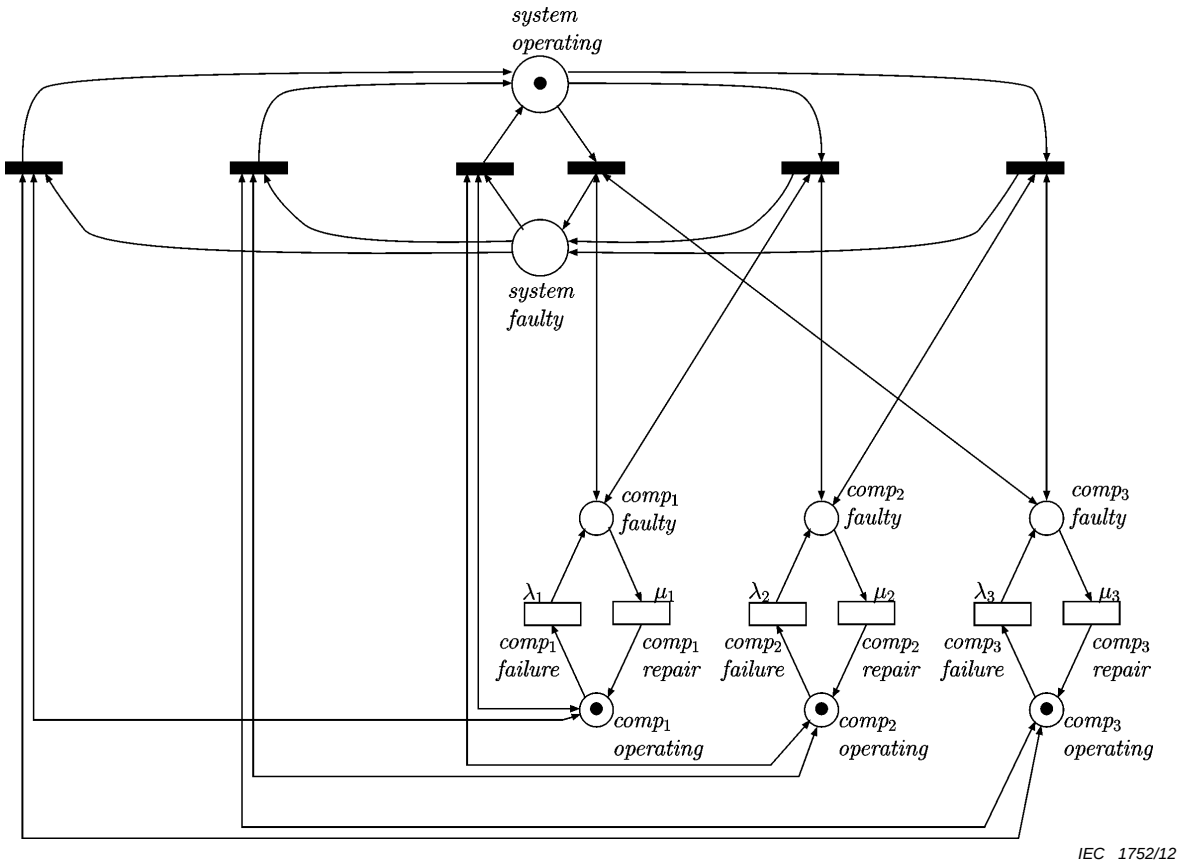


Figure B.6 – Specifically connected 2-out-of-3 availability net

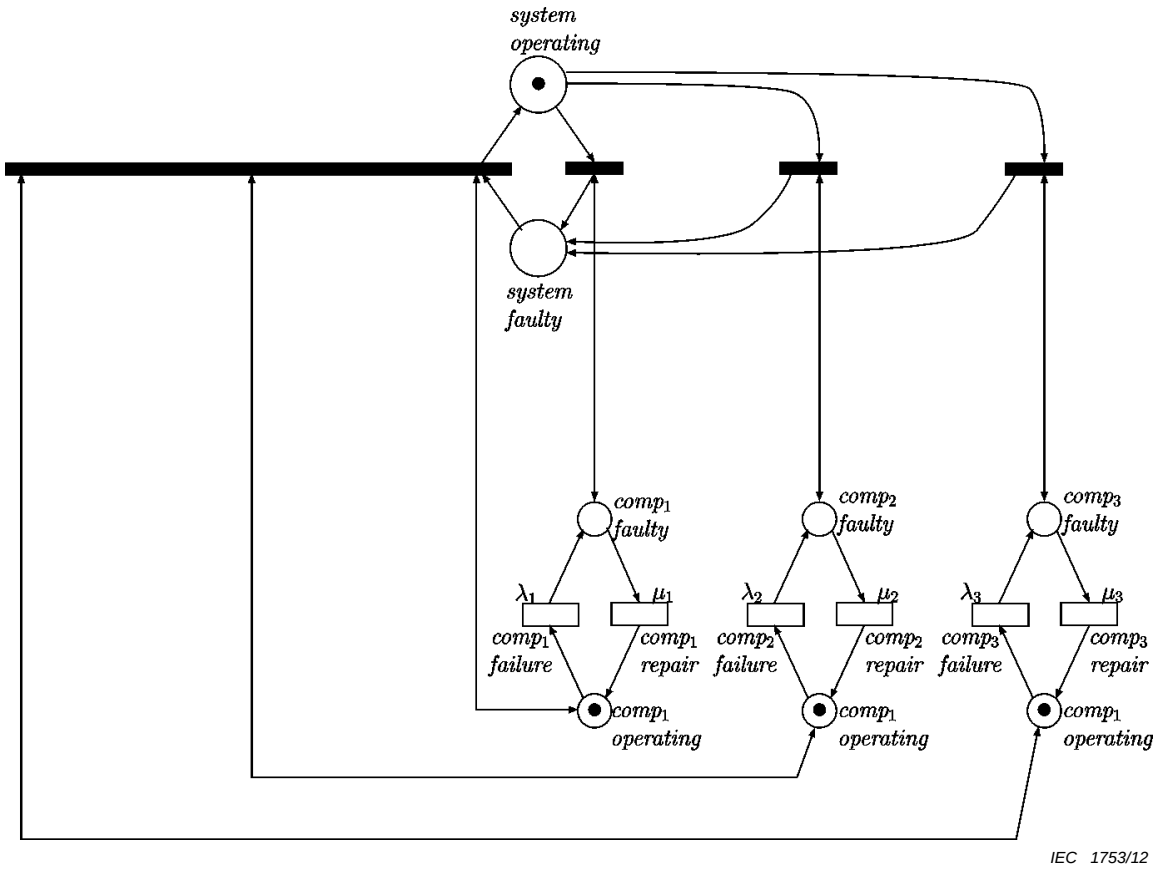


Figure B.7 – Specifically connected 3-out-of-3 availability net

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 component$_1$, component$_2$ and component$_3$ are operating; in a 2/3 system, there exist four possible states, in which the system is operating.

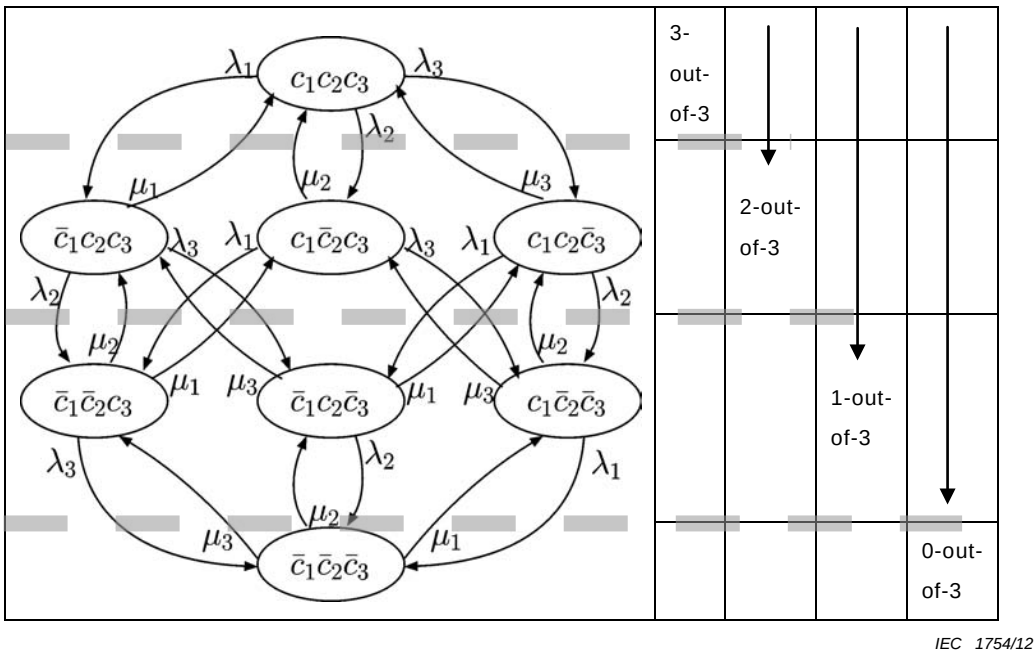


Figure B.8 – Stochastic reachability graph with system specific operating states

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.

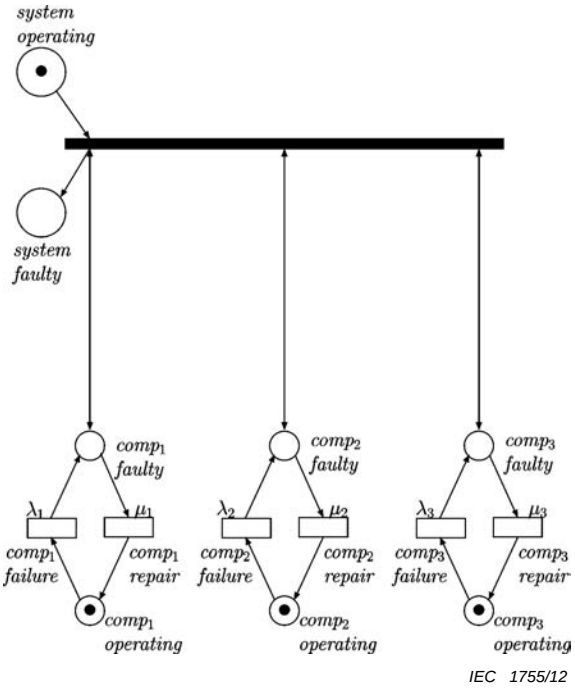


Figure B.9 – Specifically connected 1-out-of-3 reliability net

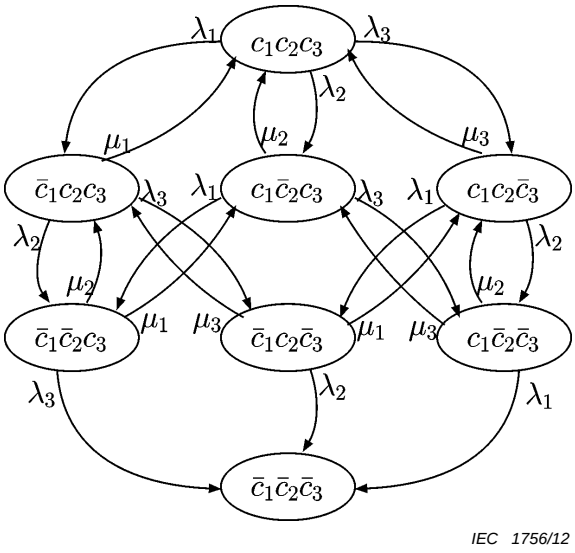


Figure B.10 – Reachability graph for the net in Figure B.9

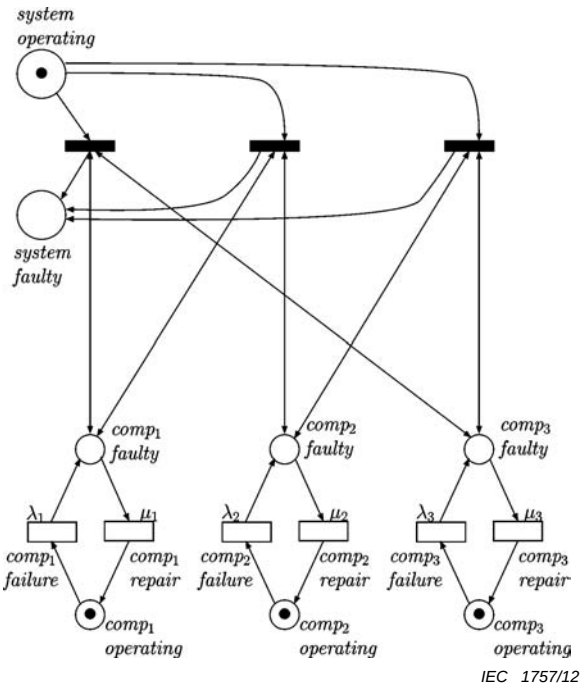


Figure B.11 – Specifically connected 2-out-of-3 reliability net

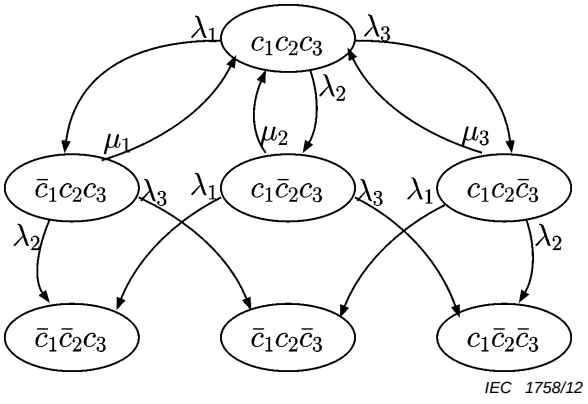


Figure B.12 – Reachability graph for the net in Figure B.11

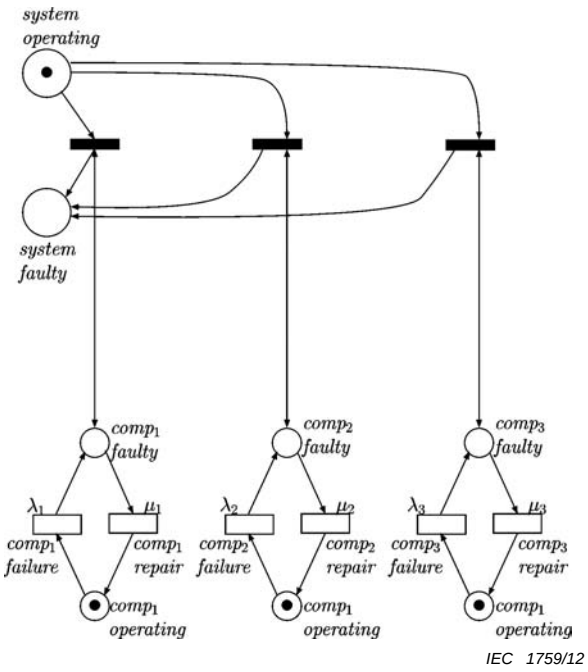


Figure B.13 – Specifically connected 3-out-of-3 reliability net

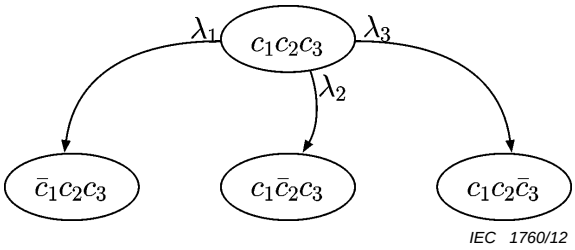


Figure B.14 – Reachability graph for the net in Figure B.13

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.

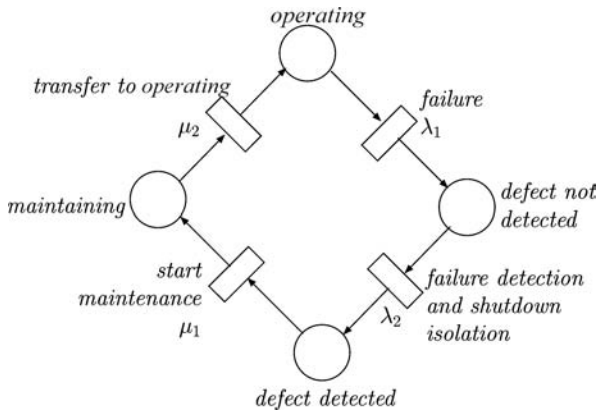
With regard to availability and maintainability, the different conditions of an item of a system to perform a function can be modelled in more detail by an extended circular Petri net (see Figure C.1) which incorporates the item's different states. These are, for example:

- 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:

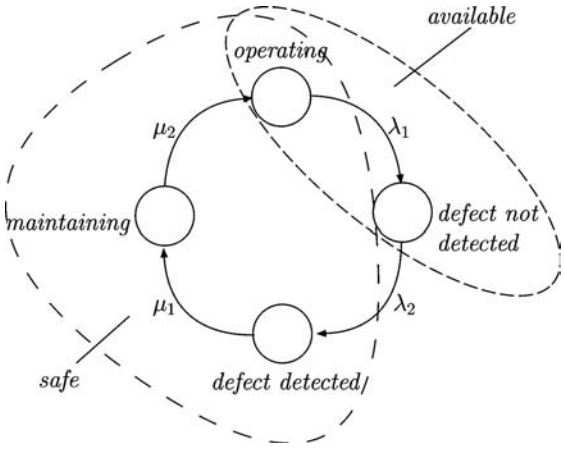
- failure event;
- failure detection and stop or shut down;
- start maintenance;
- transfer to operating state.

Note that the last three places and their interconnected transitions could be condensed to a superplace which equals the one "comp$_1$faulty" 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:

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

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

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

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).

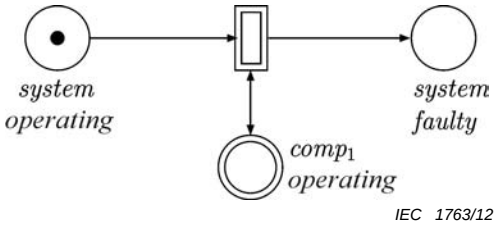


Figure C.3 – Basic reliability and function modelling concept

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.

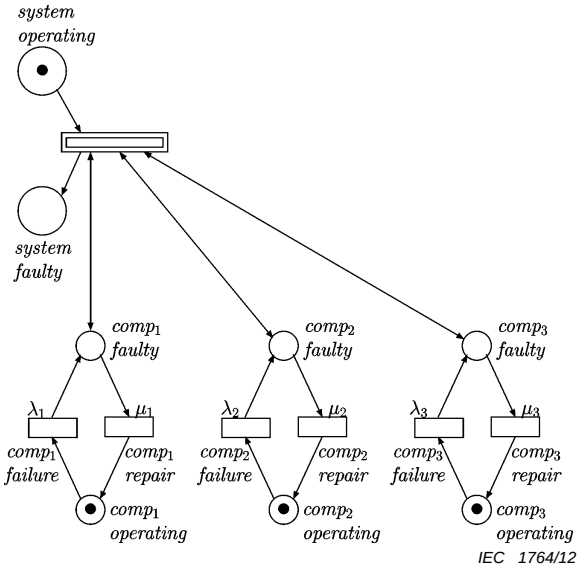


Figure C.4 – General hierarchical net with supertransitions to model reliability

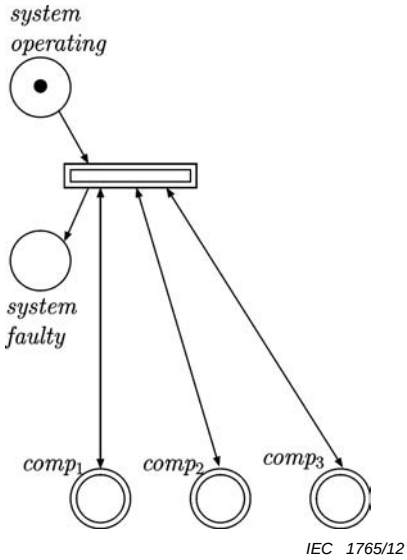


Figure C.5 – General hierarchical net with supertransitions and superplaces

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

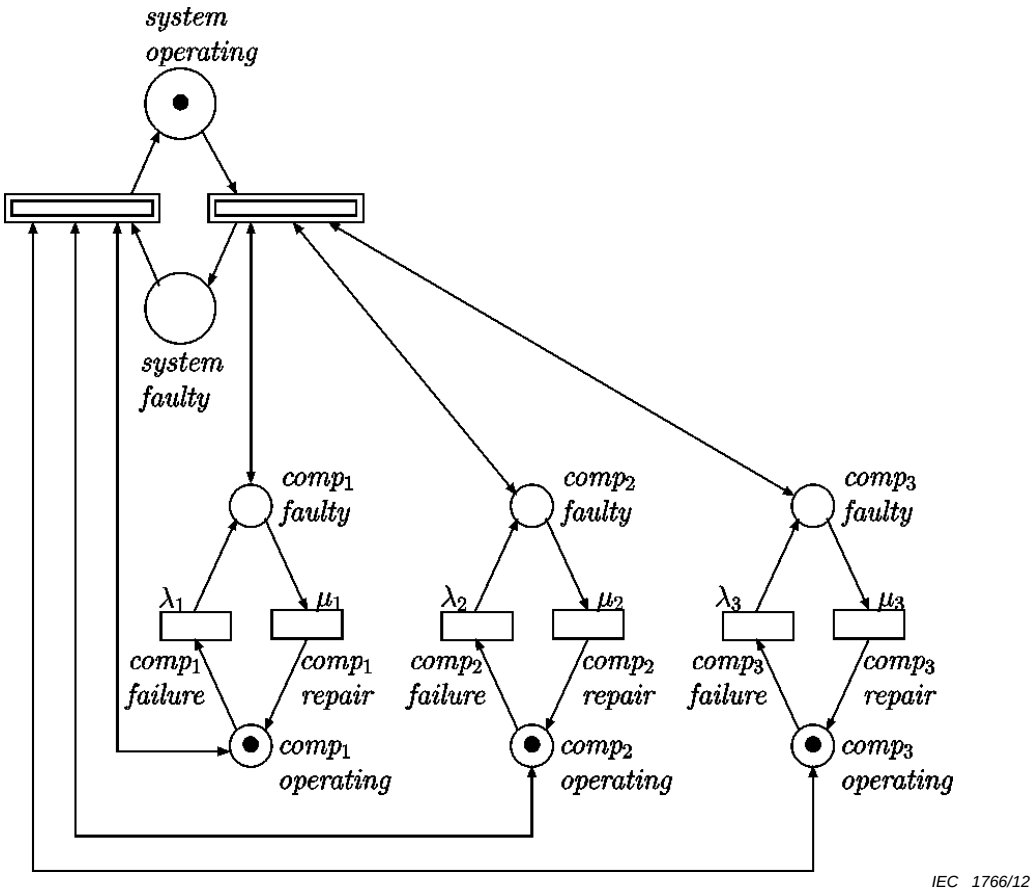


Figure C.6 – General hierarchical net with supertransitions to model availability

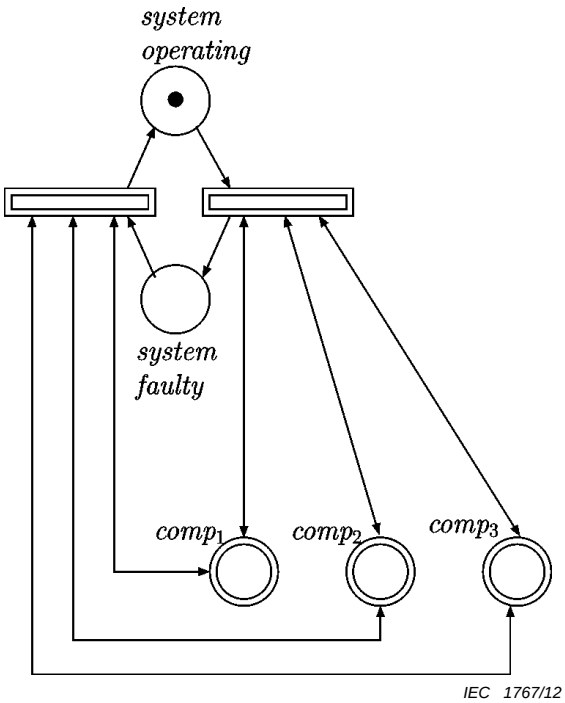


Figure C.7 – General hierarchical net with supertransitions and superplaces

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

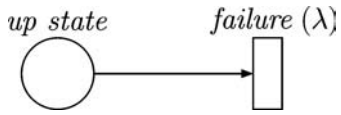
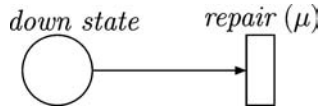
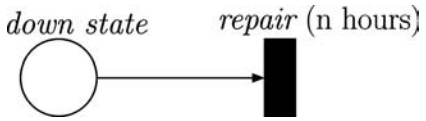
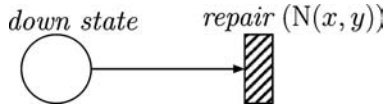
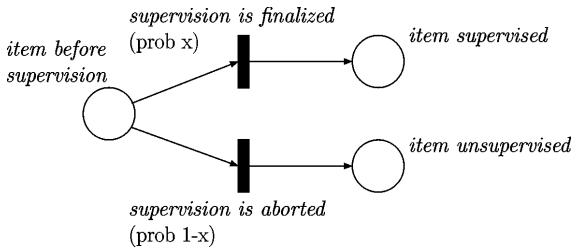
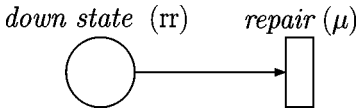
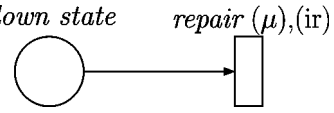
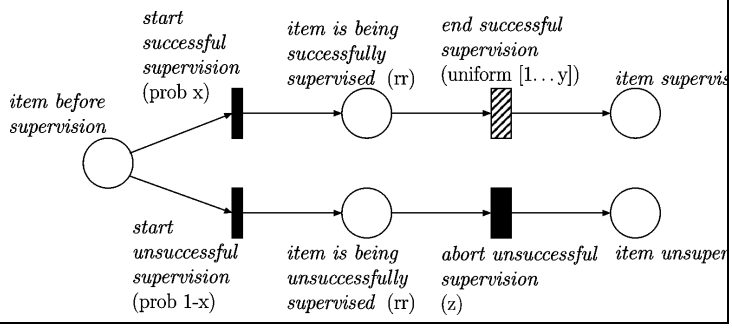
Dependability concept	PN modelling solution
Failure with constant failure rate λ (leading to exponentially distributed times to failure)	
Repair or recovery with constant rate μ leading to exponentially distributed repair/recovery times)	
Repair or recovery with a fixed repair time of n time units)	
Repair or recovery (with a truncated normal distributed repair time with a mean of x and a standard deviation of y)	
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,∞] 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.

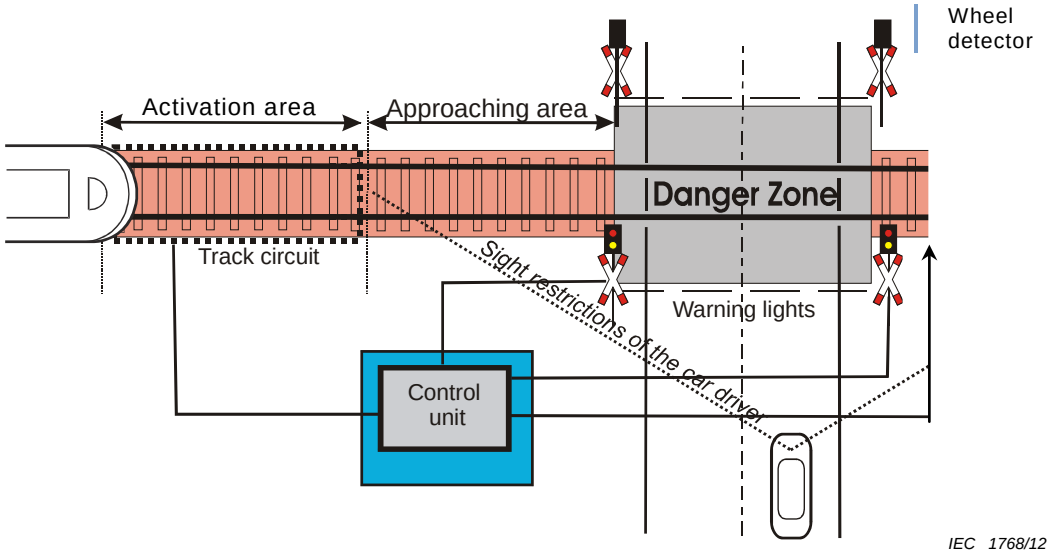


Figure E.1 – Applied example of a level crossing and its protection system

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.

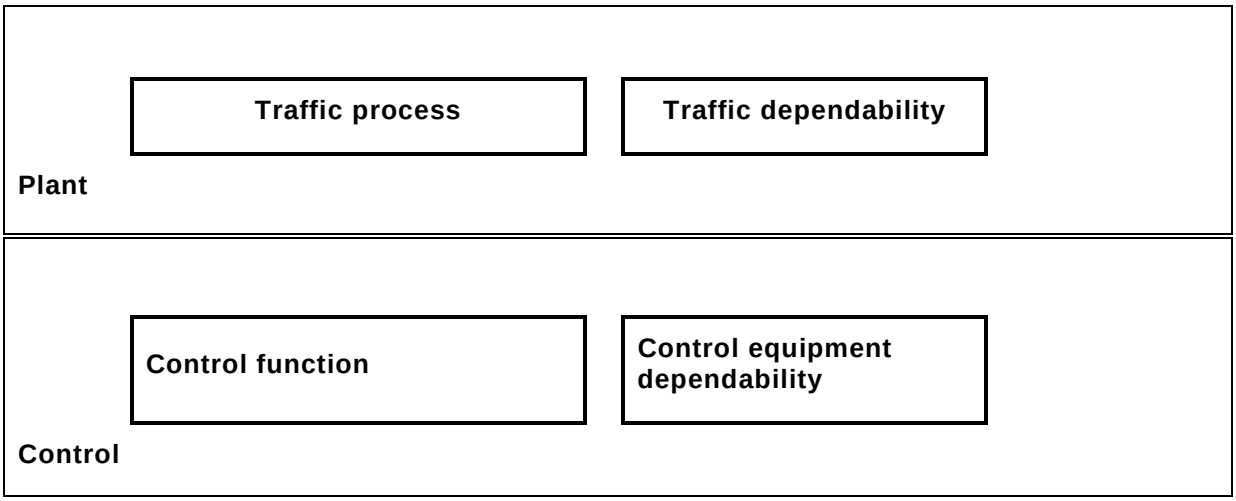
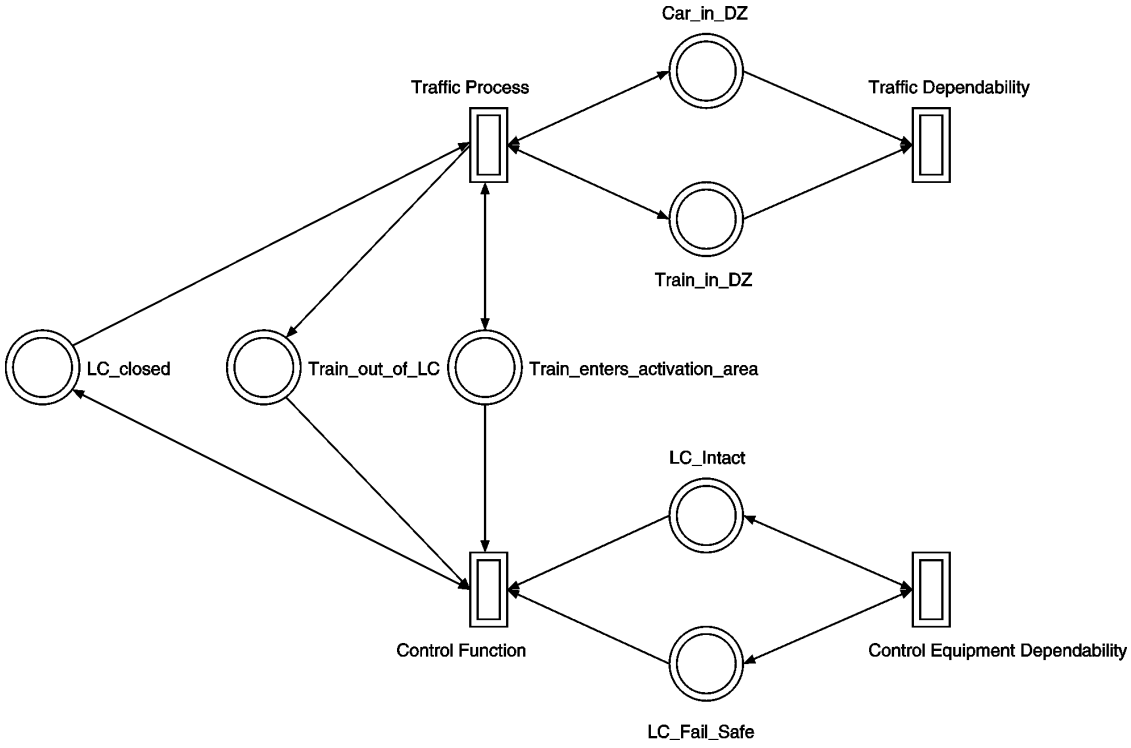


Figure E.2 – Main parts of the level crossing example model

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.



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 devide 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.

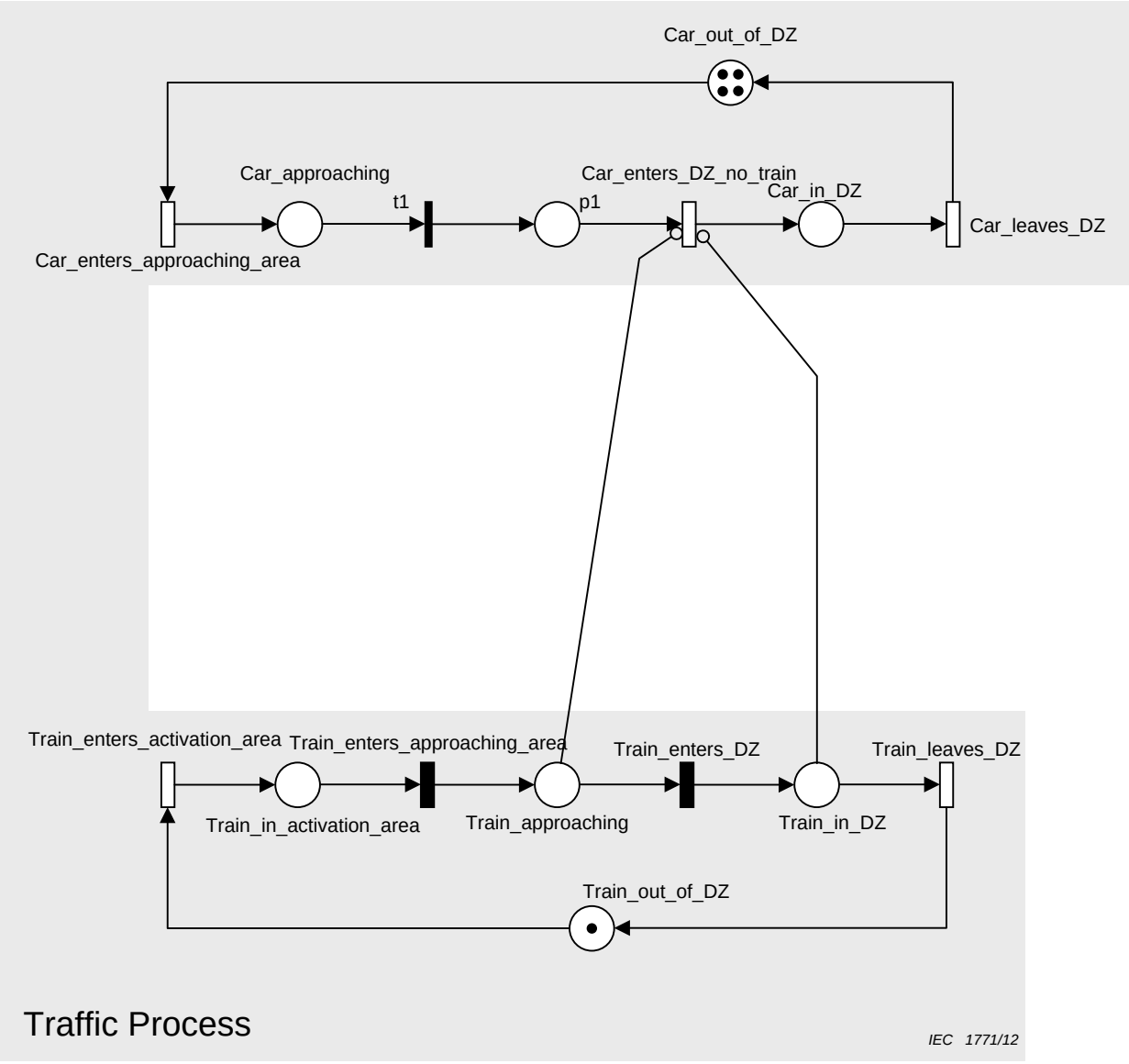


Figure E.4 – PN model of car and train traffic processes

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.

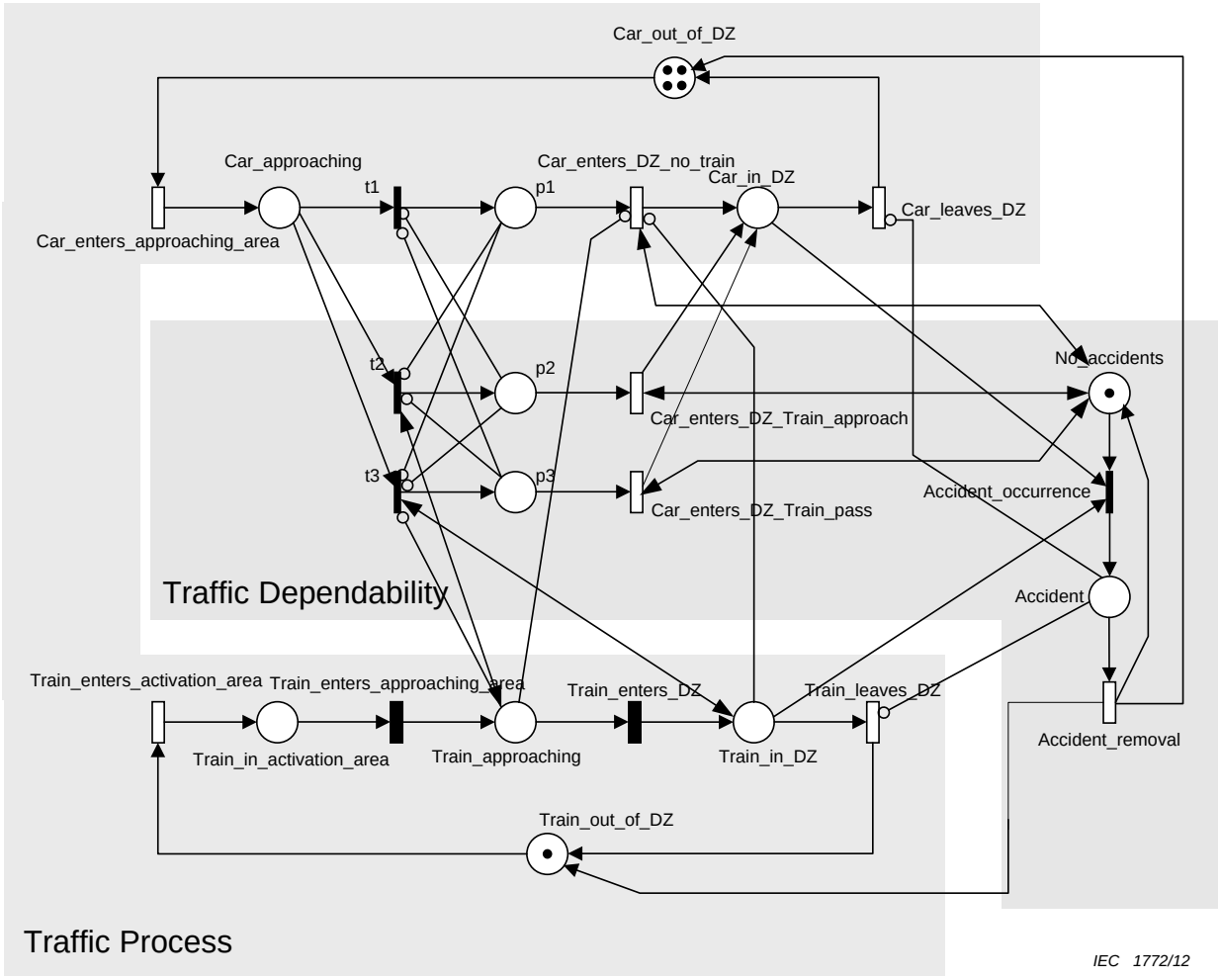


Figure E.5 – PN model of the traffic processes and traffic dependability

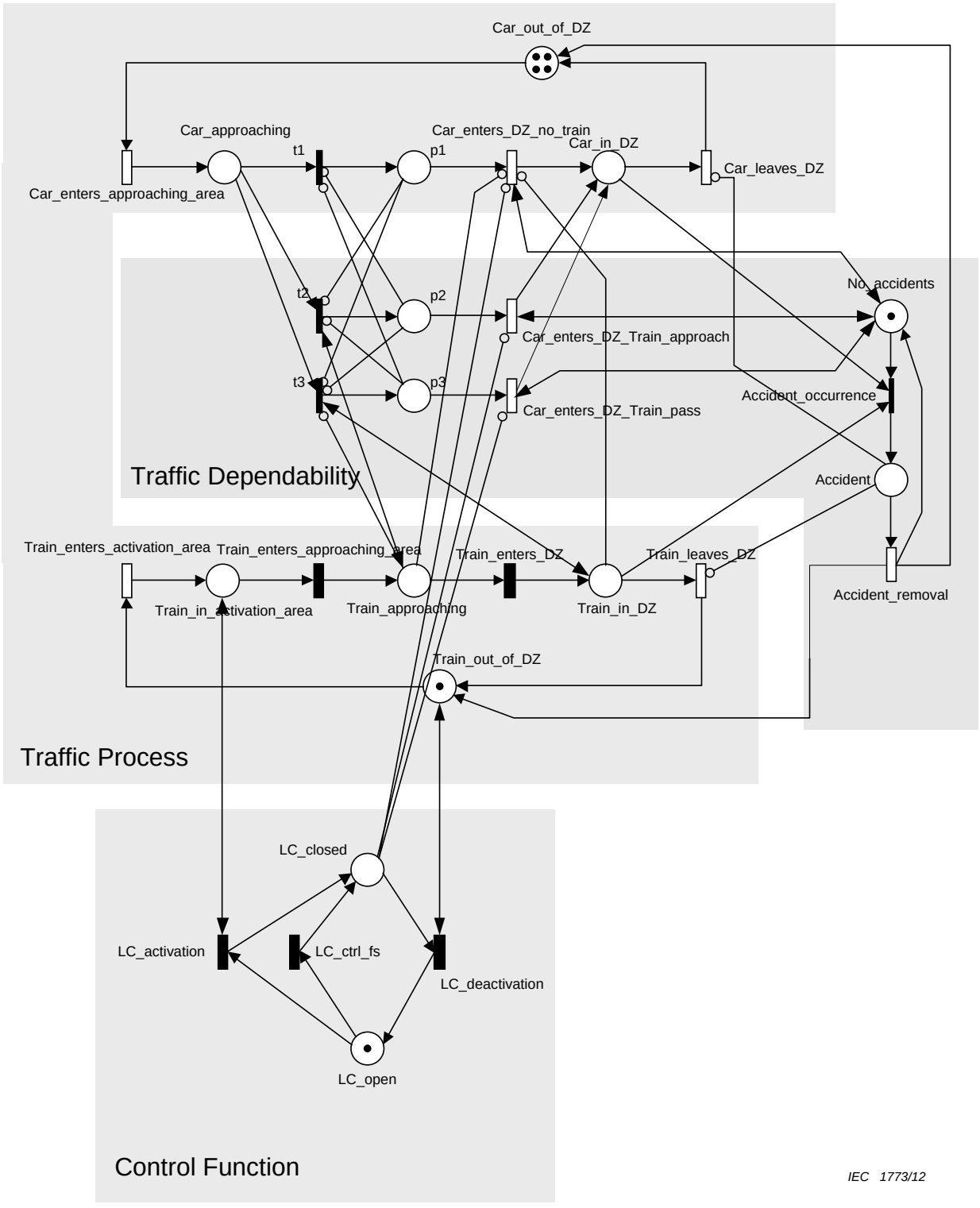


Figure E.6 – PN model of the traffic process with an ideal control function

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.

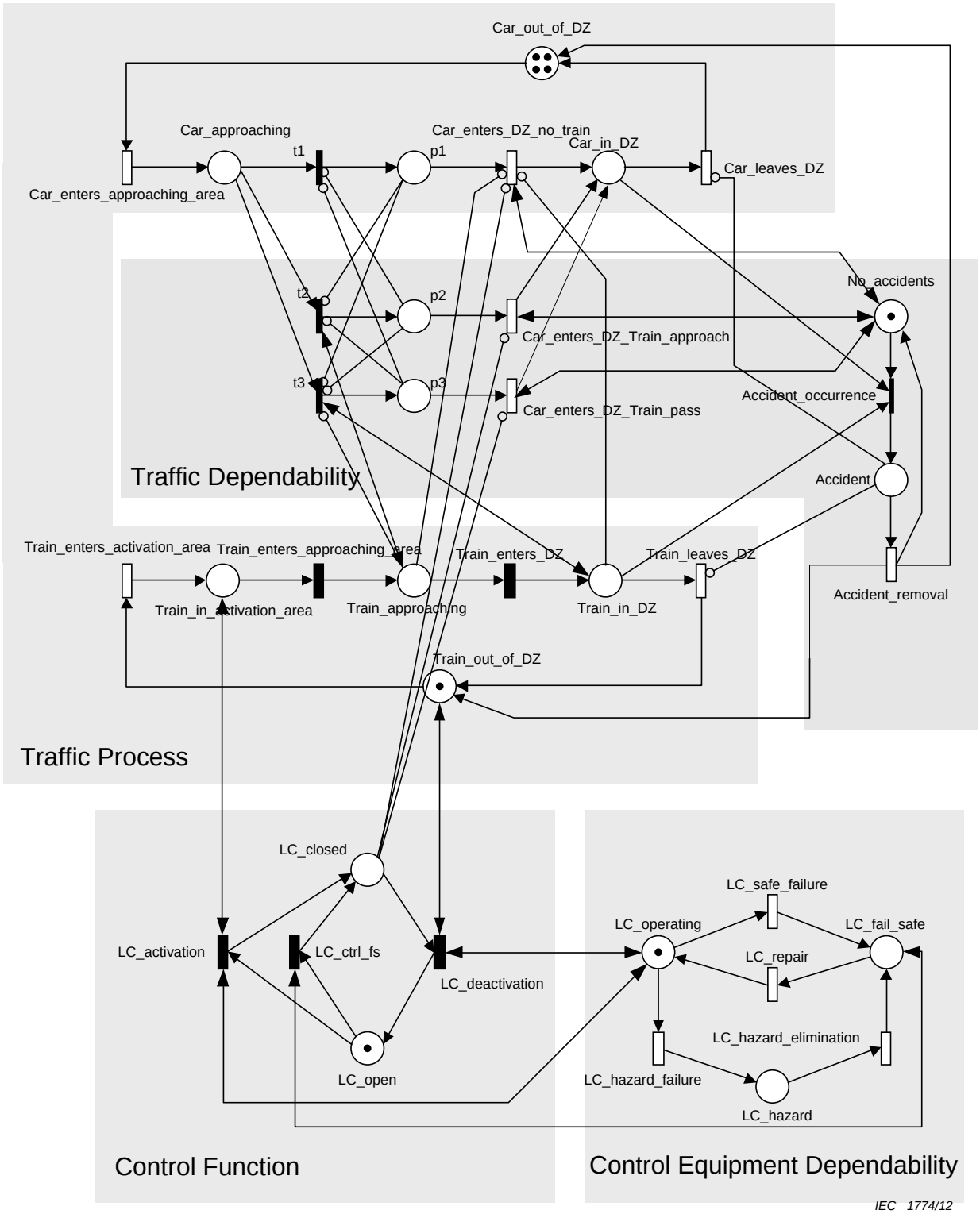


Figure E.7 – PN model of the level crossing example model

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
$p1$	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 '$p1$' 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.

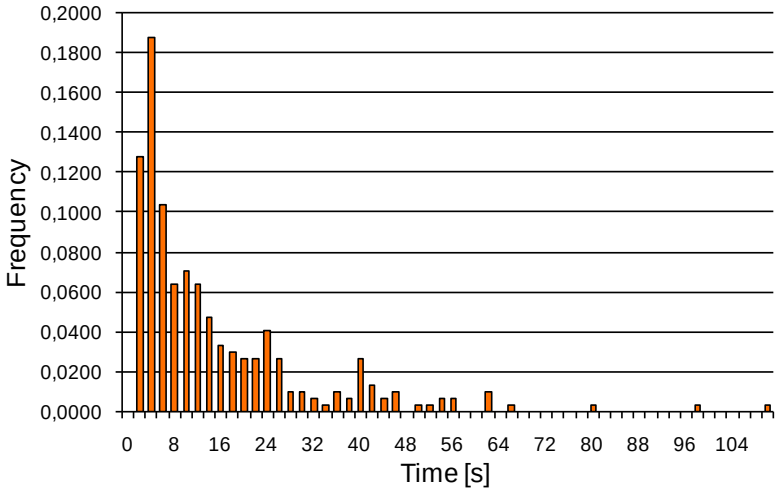


Figure E.8 – Collected measures of the road traffic flow of a particular level crossing: Time intervals between two cars coming to the level crossing

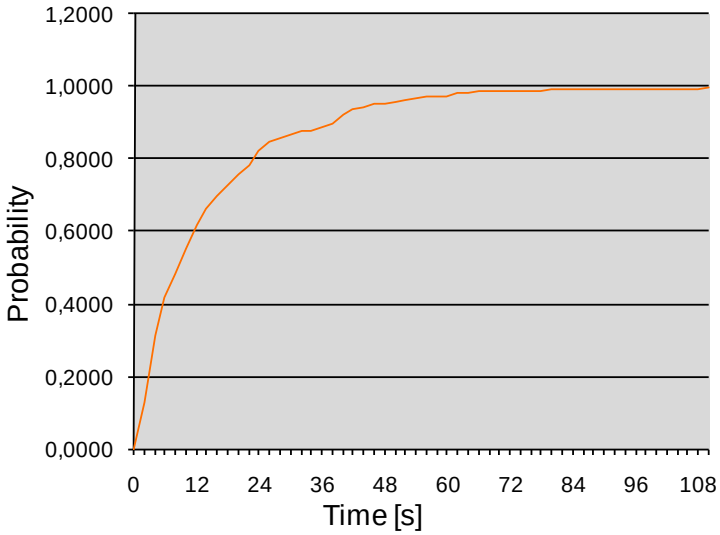


Figure E.9 – Approximated probability distribution function based on the measures depicted in Figure E.5

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.

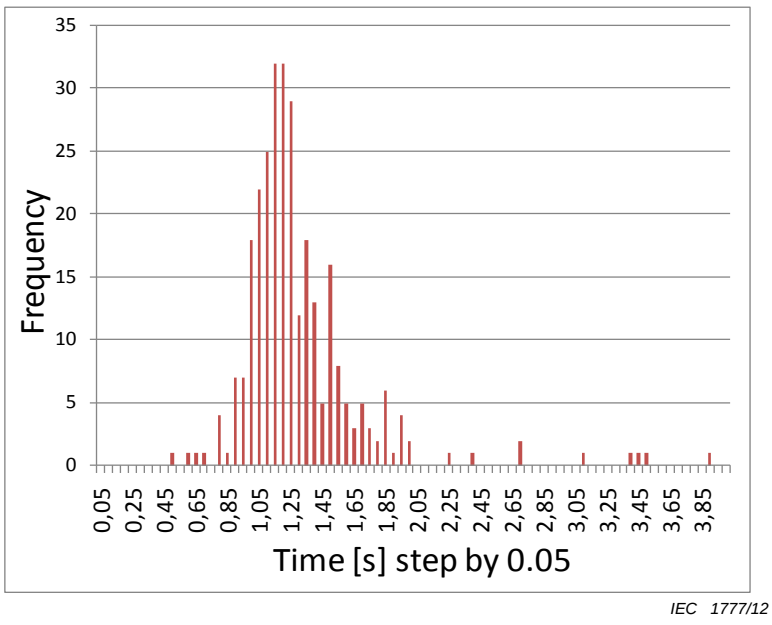


Figure E.10 – Collected measurements of time spent by road vehicle in the danger zone of the level crossing

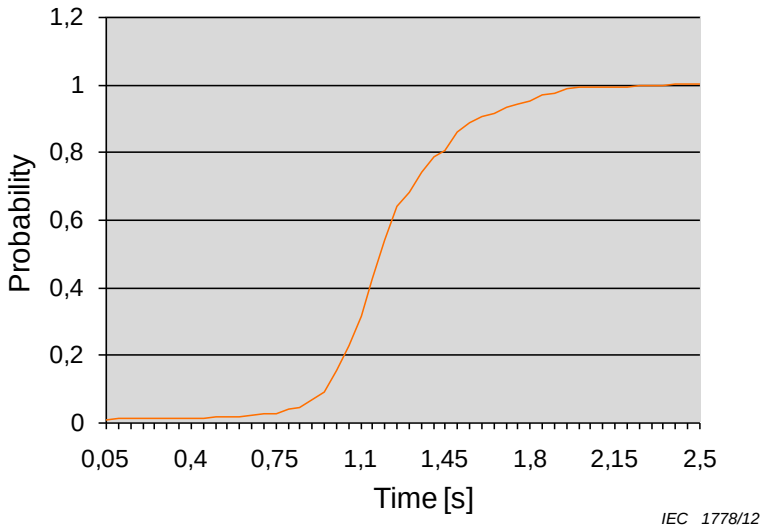


Figure E.11 – Approximated probability distribution function based on measurements depicted in Figure E.10

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)
$t1$	Immediate	95	–	Describes the case of a road vehicle entering the danger zone only if there is no train
t 2	Immediate	95	–	Describes the case of a road vehicle entering the danger zone if a train is approaching and no warning is given
$t3$	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} = const.= 0,133 min + 0,166 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 Represention 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.

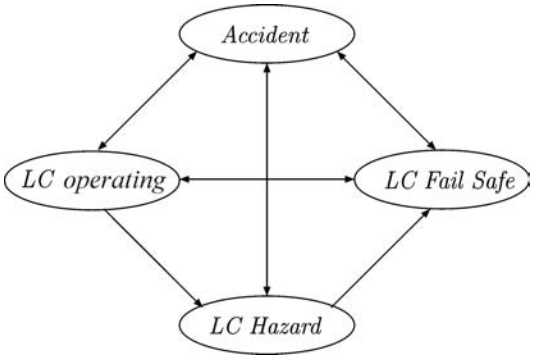


Figure E.12 – Aggregated RG and information about the corresponding states

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(accident) >= 1	39
LC operating	m(LC_operating) >= 1 ∧m(accident) = 0	71
LC Hazard	m(LC_hazard) >= 1 ∧m(accident) = 0	100
LC Fail Safe	m(LC_fail_safe) >= 1 ∧m(accident) = 0	90
NOTE '∧' specifies the logical 'and'; m(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.

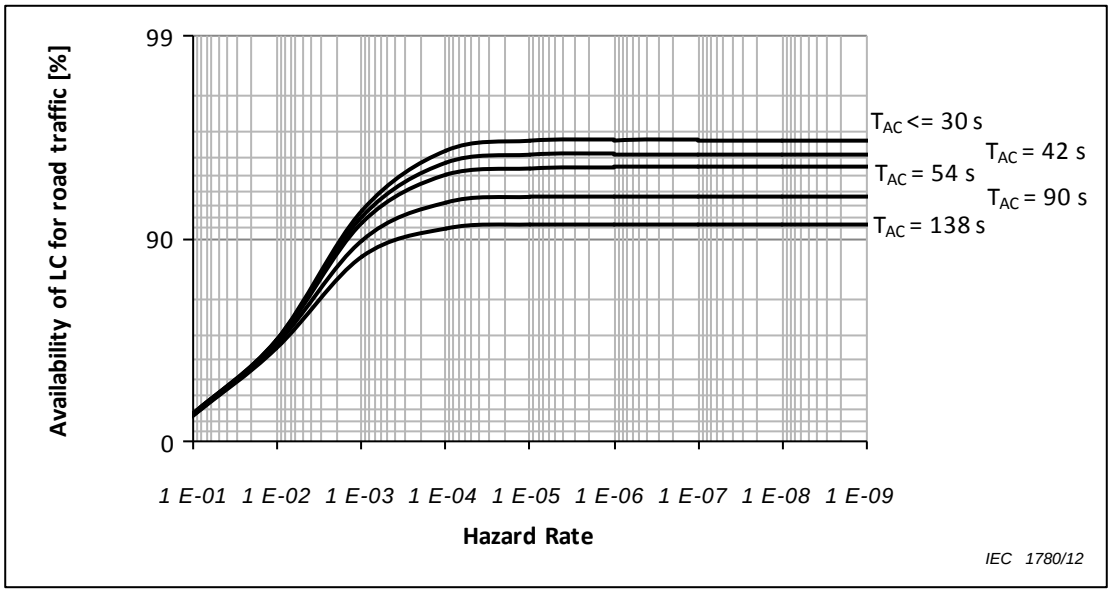


Figure E.13 – Results of the quantitative analysis showing the level crossing average availability for road traffic users as a function of the protection equipment hazard rate for different used activation and approaching times T_{AC}

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.

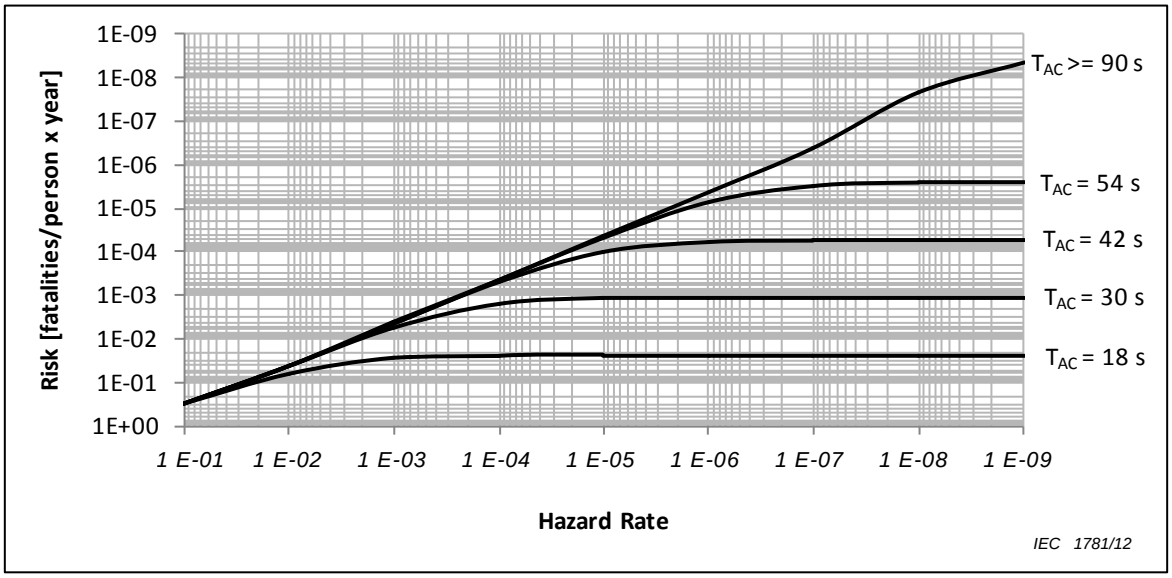


Figure E.14 – Results of the quantitative analysis showing the individual risk of the level crossing users as a function of the protection equipment hazard rate for different used activation and approaching times T_{AC}

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.

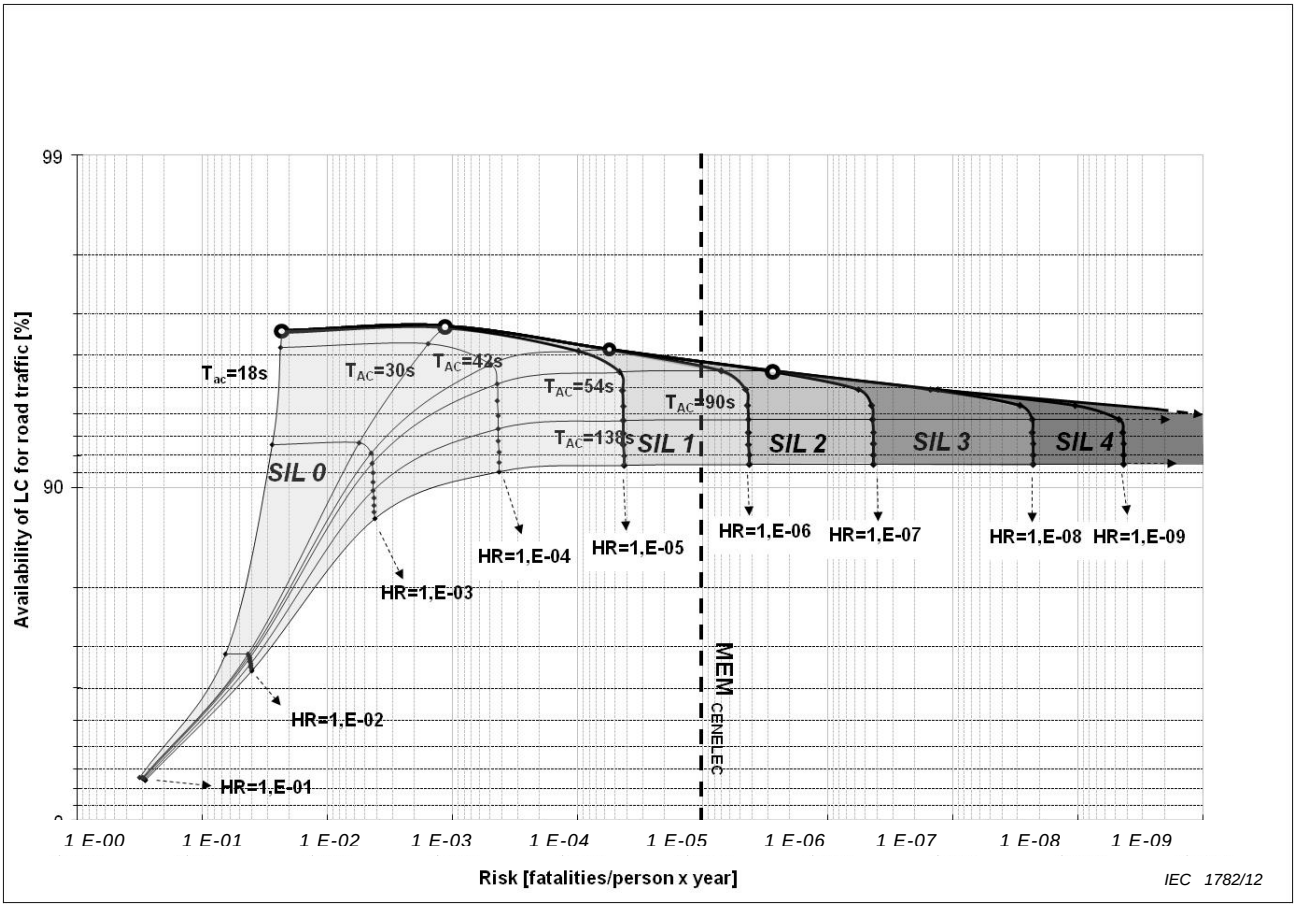


Figure E.15 – Availability safety diagram based on the quantitative results of the model analysis shown in Figure E.13 and Figure E.14

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 abbreviations*[2]

[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 stochastical 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

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

TECHNIQUES D'ANALYSE DE SÛRETÉ DE FONCTIONNEMENT – TECHNIQUES DES RÉSEAUX DE PETRI

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de brevet. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale CEI 62551 a été établie par le comité d'études 56 de la CEI: Sûreté de fonctionnement.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
56/1476/FDIS	56/1484/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

La présente Norme internationale fournit une méthode de base pour représenter les éléments de base des réseaux de Petri (PN) [1][1] et donne des directives d'application de ces techniques dans le domaine de la sûreté de fonctionnement.

La puissance intrinsèque de la modélisation par réseaux de Petri réside dans sa possibilité de décrire le comportement d'un système en modélisant la relation entre des états locaux et des événements locaux. Dans ce contexte, les réseaux de Petri sont désormais largement utilisés dans un grand nombre de domaines d'application industriels, par exemple, l'information, la communication, le transport, la production, l'industrie du traitement et de la fabrication, ainsi que l'ingénierie de l'énergie.

Les méthodes classiques (par exemple, un arbre de défaillance ou des schémas fonctionnels de fiabilité) sont très limitées lorsqu'on traite des systèmes industriels réels, car elles ne sont capables ni de traiter des systèmes à plusieurs états, ni de modéliser le comportement dynamique d'un système et peuvent faire l'objet d'une explosion combinatoire des états à traiter (par exemple, processus de Markov). Une autre modélisation et d'autres méthodes de calcul sont donc nécessaires.

Les calculs de sûreté de fonctionnement d'un système industriel ont pour but de modéliser les divers états du système et la façon dont il évolue d'un état à un autre lorsque surviennent des événements (défaillances, réparations, essais périodiques, nuit, jour, etc.).

Les ingénieurs fiabilité ont besoin d'un support graphique convivial pour réaliser leurs modèles. Grâce à leur présentation graphique, les réseaux de Petri constituent une technique de modélisation très prometteuse pour la modélisation et les calculs de sûreté de fonctionnement.

Les calculs analytiques sont limités aux petits systèmes et/ou par des hypothèses fortes (par exemple, lois exponentielles, faibles probabilités) à satisfaire. Un accroissement qualitatif est nécessaire pour traiter des systèmes à une échelle industrielle. Celui-ci peut être effectué en passant d'un calcul analytique à une simulation de Monte-Carlo.

La présente norme a pour objet de définir les principes de base consolidés des PN dans le contexte de la sûreté de fonctionnement et de l'utilisation courante de la modélisation et de l'analyse du réseau de Petri PN (*Petri net*), en tant que moyen d'évaluation qualitative et quantitative de la sûreté de fonctionnement et des mesures liées au risque d'un système.

---

1 Les chiffres entre crochets se réfèrent à la bibliographie.

TECHNIQUES D'ANALYSE DE SÛRETÉ DE FONCTIONNEMENT – TECHNIQUES DES RÉSEAUX DE PETRI

1 Domaine d'application

La présente Norme internationale donne des directives pour une technique basée sur les réseaux de Petri dans le domaine de la sûreté de fonctionnement. Elle porte sur la modélisation d'un système, l'analyse du modèle et la présentation des résultats de l'analyse. Cette méthode est orientée vers les mesures relatives à la sûreté de fonctionnement avec toutes les caractéristiques associées, telles que la fiabilité, la disponibilité, la disponibilité de production, la maintenabilité et la sécurité (par exemple, les mesures associées au niveau d'intégrité de sécurité (SIL) [2])[2].

La présente norme traite les sujets suivants en relation avec les réseaux de Petri:

a) définition des termes et symboles essentiels, description de leur utilisation et des méthodes de représentation graphique;

b) aperçu de la terminologie et de sa relation avec la sûreté de fonctionnement;

c) présentation d'une approche pas-à-pas pour

   1) la modélisation de la sûreté de fonctionnement avec des réseaux de Petri,

   2) un guide d'utilisation des techniques basées sur les réseaux de Petri pour des analyses qualitatives et quantitatives de la sûreté de fonctionnement,

   3) la représentation et l'interprétation des résultats des analyses;

d) un aperçu de la relation des réseaux de Petri avec d'autres techniques de modélisation;

e) la présentation d'exemples pratiques.

La présente norme ne donne aucune directive concernant la manière de résoudre des problèmes mathématiques apparaissant lors de l'analyse d'un PN; ces directives figurent dans les ouvrages cités en [3] et [4].

La présente norme est applicable à toutes les industries dans lesquelles des analyses qualitatives et quantitatives de sûreté de fonctionnement sont effectuées.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60050-191:1990, *Vocabulaire Électrotechnique International – Chapitre 191: Sûreté de fonctionnement et qualité de service*

3 Termes, définitions, symboles et abréviations

Pour les besoins du présent document, les termes et définitions donnés dans la CEI 60050-191 s'appliquent, ainsi que les termes et définitions suivants.

---

2 SIL: *en anglais* system integrity level

3.1 Termes et définitions

3.1.1
composant
partie constitutive d'un dispositif ne pouvant être fractionnée matériellement sans perdre sa fonction particulière

[SOURCE: CEI 60050-151:1990, 151-11-21] [5]

3.1.2
événement
quelque chose qui se produit dans le temps

Note 1 à l'article: En physique pure, un événement est considéré comme un point dans l'espace-temps.

[SOURCE: CEI 60050-111, Amendement 1:2005, 111-16-04] [6]

3.1.3
système
ensemble d'éléments reliés entre eux, considéré comme un tout dans un contexte défini et séparé de son environnement

Note 1 à l'article: Un système est en général défini en vue d'atteindre un objectif déterminé, par exemple, en réalisant une certaine fonction.

Note 2 à l'article: Les éléments d'un système peuvent être aussi bien des objets matériels, naturels ou artificiels, que des modes de pensée et les résultats de ceux-ci (par exemple, des formes d'organisation, des méthodes mathématiques, des langages de programmation).

Note 3 à l'article: Le système est considéré comme séparé de l'environnement et des autres systèmes extérieurs par une surface imaginaire qui coupe les liaisons entre eux et le système.

Note 4 à l'article: Il convient de qualifier le terme «système» lorsque le concept ne résulte pas clairement du contexte, par exemple, système de commande, système colorimétrique, système d'unités, système de transmission.

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

3.1.4
niveau d'intégrité de sécurité
SIL
niveau discret (parmi quatre possibles) correspondant à une gamme de valeurs d'intégrité de sécurité, où le niveau d'intégrité de sécurité 4 est le niveau d'intégrité de sécurité le plus haut et le niveau d'intégrité de sécurité 1 est le plus bas

Note 1 à l'article: Les mesures de défaillance cibles (voir le 3.5.17 de la CEI 61508-4:2010 [8] pour les quatre niveaux d'intégrité de sécurité sont spécifiées dans les Tableaux 2 et 3 de la CEI 61508-1:2010 [9].

[SOURCE: CEI 61508-4:1998, 3.5.8, modifiée]

3.1.5
réseau de Petri
PN
graphe biparti avec deux types de nœuds, places et transitions et arcs dirigés, destinés à modéliser respectivement des états locaux et des événements locaux

Note 1 à l'article: Les réseaux de Petri sont souvent utilisés pour modéliser le comportement de systèmes distribués.

3.1.6
arc dirigé
liaison orientée d'une paire de nœuds représentée par une ligne dotée d'une flèche

Note 1 à l'article: Les arcs dans les réseaux de Petri sont généralement dirigés. Ils ne peuvent relier que deux types de nœuds différents.

Note 2 à l'article: Outre les arcs dirigés, il existe d'autres représentations.

3.1.7
place
dans un réseau de Petri, type de nœud destiné à modéliser des états locaux ou conditions locales

3.1.8
transition
dans un réseau de Petri, type de nœud destiné à modéliser des événements locaux, c'est-à-dire des changements d'état

3.1.9
type de transition
type de transition modélisant un événement particulier d'un ensemble d'événements appartenant à une classe

Note 1 à l'article: Il existe généralement divers types de transitions dans un réseau de Petri, par exemple en vue de modéliser des événements causaux, de modéliser des événements ayant lieu après un certain retard de temps, etc

3.1.10
supernœud
dans un réseau de Petri, type de nœud destiné à cacher des sous-réseaux, particulièrement utilisé dans des modèles avec des hiérarchies

3.1.11
superarc
dans un réseau de Petri, type d'arc destiné à cacher les diverses liaisons de deux supernœuds

Note 1 à l'article: Ces deux supernœuds cachent deux sous-réseaux pouvant être reliés avec divers types d'arcs.

3.1.12
graphe d'atteignabilité
RG
diagramme de transitions d'états représentant le comportement d'un système

Note 1 à l'article: Le graphe d'atteignabilité peut être généré en se basant sur un réseau de Petri avec un marquage initial.

3.1.13
marquage
représentation graphique de l'état du système modélisé par un réseau de Petri

3.2 Symboles et abréviations

NOTE La représentation graphique d'un réseau de Petri nécessite des symboles, identifiants et étiquettes qu'il convient d'utliser d'une manière cohérente. Un récapitulatif de représentations graphiques couramment utilisées est indiquée dans le Tableau 1, le Tableau 2 et le Tableau 3.

Les symboles suivants du Tableau 1 sont recommandés dans les réseaux de Petri non synchronisés. L'étiquette «n» de l'arc normal spécifie une valeur entière.

Tableau 1 – Symboles des réseaux de Petri non synchronisés

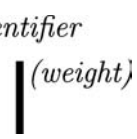
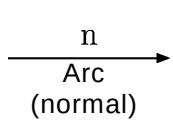
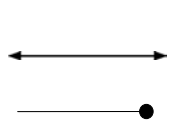
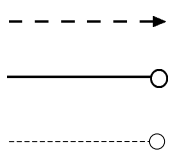
						
Symbole de place également utilisé pour des places multiples	Symbole de transition	Symbole de transition avec un poids de transition	Symboles de relation – arcs normaux	Symboles de relation – arcs d'essai	Symboles de relation – arcs inhibiteurs	Symbole de jeton
Il existe plusieurs possibilités pour dessiner des arcs d'essai et des arcs inhibiteurs. Le symbole de jeton n'est pas un symbole de la structure statique du réseau mais il est utilisé pour symboliser le flux d'informations.						

Tableau 2 – Symboles supplémentaires des réseaux de Petri synchronisés

	Type de transition			
	Déterministe		**Stochastique**	
	Retard nul	Retard d	Distribué de façon exponentielle ou géométrique	Distribué arbitrairement
Paramètre		d	λ	∅ Distribution arbitraire
Symbole				
NOTE En cas de transitions déterministes, on utilise souvent une distribution de Dirac. De plus, les paramètres d'une transition synchronisée peuvent dépendre de l'état ou du temps.				

Tableau 3 – Symboles pour une modélisation hiérarchique

Identifiant 	*Identifiant* 	*Identifiant* 	
Symbole de superplace	Symbole de supertransition	Symbole de supernœud	Symbole de superarc
Noter que le symbole d'un «superarc» n'a pas de direction, car il peut remplacer plusieurs arcs avec des directions différentes.			

Abréviation	**Explication**
CDF	Fonction de distribution cumulative (en anglais *Cumulative distribution function*)
AAE	Analyse par arbre d'événement (en anglais *Event tree analysis*)
DZ	Zone de danger (en anglais *Danger zone*)
AMDE (C)	Analyse des modes de défaillance et de leurs effets (criticité) (en anglais *Failure, mode, effects (and criticality) analysis*)
AAP	Analyse par arbre de panne (en anglais *Fault tree analysis*)
HR	Taux de danger (en anglais *Hazard rate*)

LC	Passage à niveau (en anglais *Level crossing*)
MTBF	Temps moyen entre défaillances (*Mean time between failures)*
MTTF	Moyenne des temps avant défaillance (*Mean time to failure)*
PN	Réseau de Petri (en anglais *Petri net*)
BDF	Bloc-diagramme de fiabilité (en anglais *Reliability block-diagram*)
RG	Graphe d'atteignabilité (en anglais *Reachability graph*)
SIL	Niveau d'intégrité de sécurité (en anglais *Safety integrity level*)
ir	Récompense impulsionnelle (en anglais *Impulse reward*)
rr	Taux de récompense (en anglais *Rate reward*)

4 Description générale des réseaux de Petri

4.1 Réseaux de Petri de bas niveau non synchronisés

Les réseaux de Petri (PN) sont des graphes dans lesquels les nœuds actifs et passifs sont différenciés. Les éléments passifs sont appelés places; ils modélisent les états locaux ou conditions locales, par exemple, et sont marqués avec des jetons si l'état local est satisfait. Les éléments actifs sont appelés transitions. Ils modélisent les changements possibles d'un état à un autre (par exemple, les événements potentiels qui peuvent survenir). Les places et les transitions peuvent être appelées nœuds. Les relations causales entre les phénomènes représentés par des places et des transitions sont décrites explicitement par divers types d'arcs dirigés qui relient ces nœuds (voir les symboles de base d'un réseau de Petri dans le Tableau 1 et l'Article A.1 pour une introduction aux PN). Les arcs inhibiteurs ne peuvent relier que des places de pré-ensemble avec des transitions dans leur post-ensemble (voir A.1.2).

Une transition est activée si toutes les places de pré-ensemble qui y sont reliées par des arcs normaux ou d'essai sont marquées avec un nombre suffisant de jetons et si toutes ses places de pré-ensemble qui y sont reliées par des arcs inhibiteurs ne sont pas marquées. Le nombre de jetons suffisants pour l'activation d'une transition est noté sur l'arc. En général, cette annotation peut dépendre du marquage (voir [3]). Voir 4.4 pour les généralisations de ces concepts couramment utilisés.

Si une transition est activée, elle peut tirer, c'est-à-dire qu'elle peut modifier le marquage du modèle. Le tir d'une transition ne modifie que le marquage des places qui y sont reliées par des arcs normaux: le tir conduit à l'absorption de jetons depuis les places correspondantes dans son pré-ensemble et à la production de jetons dans son post-ensemble. Le nombre de jetons absorbés et produits est spécifié par l'étiquette d'arc. Si aucune étiquette d'arc n'est fournie, le nombre est égal à un.

Ceci signifie que les places, les transitions et les arcs constituent les éléments statiques et les relations d'un système, tandis que les jetons peuvent être produits ou peuvent disparaître en fonction des états du système modélisé.

Le graphe d'atteignabilité d'un PN est donc constitué de tous les marquages globaux qui peuvent être atteints depuis un marquage initial par l'intermédiaire d'une séquence arbitraire de tirs de transition. Sur ce graphe, un nœud représente un marquage global individuel et chaque arc représente le tir d'une transition qui transforme un marquage global en un autre.

Les PN peuvent être représentés de façon non graphique par des matrices d'incidence. Si T est l'ensemble de transitions et P est l'ensemble de places, alors la matrice d'incidence est de dimension $|P|\times|T|$. Pour chaque transition, le changement du marquage global dû au tir est spécifié dans une colonne correspondante.

4.2 Réseaux de Petri de bas niveau synchronisés

Dans les PN synchronisés, aussi bien des transitions non synchronisées que des transitions synchronisées peuvent être utilisées. Pour effectuer un tir, une transition synchronisée doit être activée pendant une durée spécifique. Cette durée peut être déterministe ou stochastique, selon la fonction de distribution spécifique de la transition (fonction de distribution cumulative – CDF – *en anglais: cumulative distribution function*) et les paramètres correspondants. Si deux transitions ou plus sont activées en même temps, alors le tir des transitions est déterminé par une autre spécification de la transition, à savoir, la «politique de présélection» ou la «politique de course». De plus, les choix concernant la politique d'exécution et la politique de mémoire, hormis les distributions de temps de tir, doivent être spécifiés ([3]). À l'expiration de cette durée, la transition est autorisée à tirer. Le Tableau 2 représente les transitions couramment utilisées dans les PN synchronisés.

En correspondance avec le type spécifique d'une transition synchronisée, celle-ci peut être attribuée par un paramètre de temps qui spécifie la durée de temps fixe (transitions avec temps de tir déterministe), la vitesse de tir constante (transitions avec temps de tir distribué de façon exponentielle ou géométrique) ou la distribution de probabilité avec ses paramètres (transitions avec temps de tir distribués de façon arbitraire). On notera que les transitions non synchronisées sont un cas particulier de transitions de durée de tir fixe avec un retard déterministe de zéro.

Comme dans le cas non synchronisé, le RG (graphe d'atteignabilité) d'un PN est constitué de nœuds représentant les marquages globaux et de flèches représentant le tir des transitions. Outre le RG non synchronisé, le RG d'un réseau synchronisé doit tenir compte des paramètres spécifiques des transitions.

4.3 Réseaux de Petri de haut niveau

Dans les réseaux de Petri de haut niveau, un marquage est constitué de tuples individuels distinctifs au lieu de jetons noirs anonymes. Ainsi, non seulement les tuples modélisent la satisfaction des conditions ou l'existence d'états, mais également les informations elles-mêmes. Par rapport à ce contexte, les étiquettes d'arc peuvent être formulées en fonction des informations existantes. Un tel support de modélisation conduit à des modèles compacts et intuitifs, même pour des systèmes complexes. Puisque la méthode présentée dans la présente norme ne dépend pas de ces possibilités, en ce qui concerne les PN de haut niveau, on se référera à l'ISO/CEI 15909-1 (voir [10]).

4.4 Extensions des réseaux de Petri et modélisation avec des réseaux de Petri

NOTE Pour la modélisation avec des PN, certaines notations, extensions et dénominations couramment utilisées sont présentées dans ce paragraphe.

4.4.1 Autres représentations des éléments des réseaux de Petri

4.4.1.1 Généralités

En plus des symboles qui ont été présentés dans le Tableau 1, les symboles et concepts suivants pour les arcs inhibiteurs pondérés, les places multiples et les variables globales sont également couramment utilisés.

4.4.1.2 Arcs inhibiteurs pondérés

Comme pour les arcs normaux, les arcs inhibiteurs peuvent être pondérés, voir Figure 1.

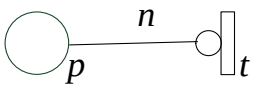


Figure 1 – Arc inhibiteur pondéré

La transition t de la Figure 1 n'est activée que si le nombre de jetons à la place p est inférieur à n. Noter que le marquage peut en réalité être inférieur, s'il y a n jetons à la place p, la transition t n'est pas activée.

Pour améliorer la lisibilité des réseaux complexes, en particulier lors de la modélisation de systèmes à une échelle industrielle, divers concepts supplémentaires sont couramment utilisés.

4.4.1.3 Places multiples

Si la même place apparaît plusieurs fois dans un réseau, ces places sont appelées «places multiples», «places répétés» ou «places de fusion». La structure modulaire d'un modèle peut ainsi être révélée. Puisque les places multiples ne sont que des copies identiques les unes des autres, leur marquage est le même dans chaque marquage du réseau.

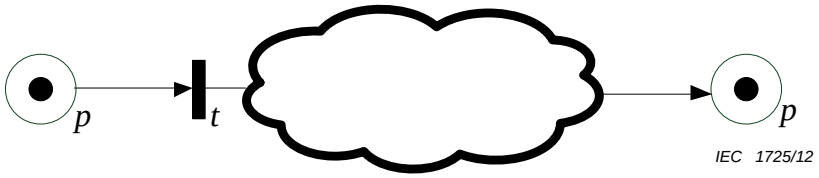


Figure 2 – La place *p* est une place multiple

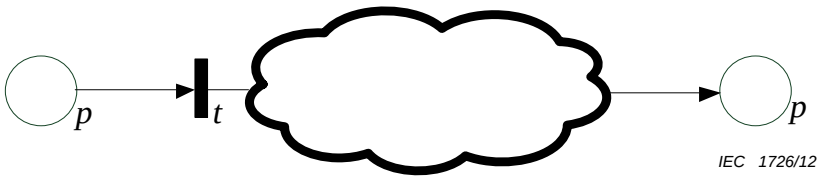


Figure 3 – Marquage sur *p* après tir de la transition *t*

4.4.1.4 Variables globales

L'utilisation des variables globales est similaire à celles des places multiples. L'activation d'une transition peut être conditionnée à la valeur de variables globales ou prédicats. De plus, le tir d'une telle transition peut changer la valeur des variables globales en utilisant des assertions et des prédicats.

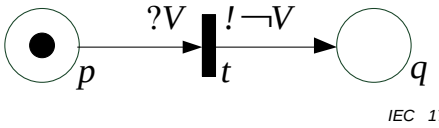


Figure 4 – L'activation de *t* dépend de la valeur de *V*

Sur le réseau de la Figure 4, la transition t dans l'état décrit est simplement activée, si la variable globale V est vraie (*?* est un opérateur de «lecture», c'est-à-dire que $?V$ sert de protection lors de la lecture de la valeur de la variable globale V). Un tir de t marque la place q, démarque la place p et met V à faux (*!* est un opérateur «d'écriture», c'est-à-dire que $!\neg V$ met la valeur de la variable globale V à faux: $\neg V$ signifie «non V»). Dans ce contexte, on parle souvent d'actions ou d'assertions de «lecture» et «d'écriture».

4.4.2 Relation avec les concepts de sûreté de fonctionnement

Les réseaux de Petri à l'échelle industrielle sont souvent modularisés dans divers sous-réseaux de Petri en communication, voir par exemple [11] et [12].

Dans le contexte de la sûreté de fonctionnement, des événements locaux, tels que des défaillances ou des réparations, peuvent être modélisés par des transitions et des états locaux, tels que des défauts, peuvent être modélisés par des places. En conséquence, le nom associé à chaque nœud représente principalement la caractéristique de sûreté de fonctionnement correspondante et indique le dispositif associé s'il est requis. Si les concepts des PN sont interprétés de cette manière, on peut parler de «PN interprétés de sûreté de fonctionnement».

Le Tableau 4 fournit une vue d'ensemble de concepts correspondants entre des systèmes en général, les réseaux de Petri et les concepts de sûreté de fonctionnement. Ce tableau ne comporte pas toutes les interprétations possibles des défaillances ou des états défectueux.

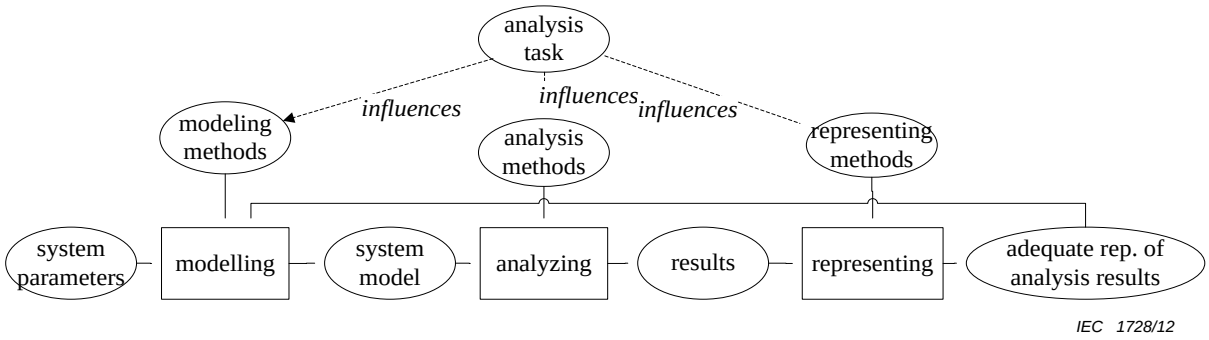
Tableau 4 – Concepts correspondants dans les systèmes, réseaux de Petri et sûreté de fonctionnement

Aspect	Système	Réseau de Petri	Sûreté de fonctionnement	
Dynamique	Événement	Transition	Défaillance	Réparation
Statique	État local	Place	Défectueux	Fonctionnel
NOTE La défaillance et la réparation ne sont que des exemples d'événements concernant la sûreté de fonctionnement; défectueux et fonctionnel ne sont que des exemples d'états concernant la sûreté de fonctionnement, d'autres exemples sont une première défaillance ou des défaillances et des états dégradés. Ces concepts peuvent être utilisés comme base pour calculer par exemple la disponibilité de production moyenne.				

5 Modélisation et analyse de la sûreté de fonctionnement par réseaux de Petri

5.1 Étapes à exécuter en général

L'analyse d'un système requiert en général un modèle de ce système détaillé de manière adéquate. Le niveau de détail requis dépend des analyses qui doivent être effectuées. Les systèmes sont généralement trop complexes pour être modélisés à un niveau détaillé dans leur totalité en une seule étape. En conséquence, la modélisation doit être effectuée de manière itérative, en démarrant d'une description textuelle grossière et en finissant par un modèle formel détaillé. Les résultats d'analyse obtenus en se basant sur le modèle doivent être représentés d'une manière conviviale et doivent être interprétés par rapport au contexte de la tâche d'analyse (voir Figure 5).

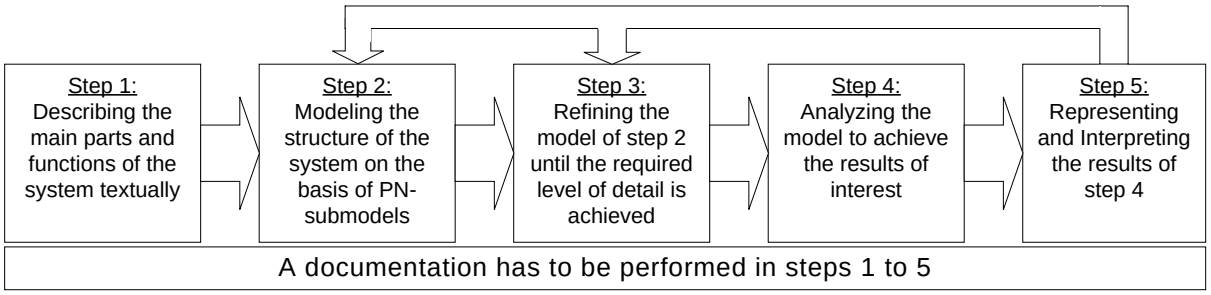


Légende

Anglais	Français
Analysis task	Tâche d'analyse
Modelling methods	Méthodes de modélisation
Influences	Influences
Analysis methods	Méthodes d'analyse
Representing methods	Méthodes de représentation
System parameters	Paramètres du système
Modelling	Modélisation
System model	Modèle du système
Analysing	Analyse
Results	Résultats
Representing	Représentation
Adequate representation of analysis results	Représentation adéquate des résultats d'analyse

Figure 5 – Méthodologie constituée principalement des étapes de «modélisation», «analyse» et «représentation»

La Figure 6 représente les principales étapes de modélisation et d'analyse de la sûreté de fonctionnement avec des PN. Bien que ressemblant à un processus direct, l'analyste doit garder à l'esprit que la modélisation est généralement principalement un processus itératif. L'Étape 3 en particulier «Précision du modèle» nécessitera plusieurs itérations.



IEC 1729/12

Légende

Anglais	Français
Step 1: Describing the main parts and functions of the system textually	Étape 1: Description des parties principales et fonctions du système, textuellement
Step 2: Modelling the structure of the system on the basis of PN-submodels	Étape 2: Modélisation de la structure du système basée sur les sous-modèles du PN
Step 3: Refining the model of step 2 until the required level of detail is achieved	Étape 3: Précision du modèle de l'étape 2 jusqu'a atteindre le niveau de détail requis
Step 4: Analysing the model to achieve the results of interest	Étape 4: Analyse du modèle pour obtenir les résultats d'intérêt
Step 5: Representing and interpreting the results of step 4	Étape 5: Représentation et interprétation des résultats de l'étape 4

Figure 6 – Processus de modélisation et d'analyse de la sûreté de fonctionnement avec des réseaux de Petri

Étape 1: Description des parties principales du système par des moyens de description classiques, par exemple textuellement, avec des tableaux et des figures, etc. (voir 5.2.2).

Étape 2: Modélisation de la structure du système en se basant sur des sous-modèles de PN et sur leurs relations et en documentant ce modèle (voir 5.2.3).

Un système est souvent constitué de deux sous-systèmes principaux:

a) l'installation, c'est-à-dire le sous-système fonctionnel devant être contrôlé;

b) le contrôle, c'est-à-dire le sous-système qui sert à contrôler l'installation.

Étape 3: Précision du modèle de l'Étape 2 jusqu'à atteindre le niveau de détail requis et documentation de ce modèle précisé (voir 5.2.4).

Une notation en PN du système de l'Étape 2 incluant les sous-systèmes doit être fournie.

Le niveau de détail requis est atteint lorsque toutes les informations nécessaires pour les analyses sont incluses dans le modèle.

Étape 4: Analyse du modèle pour obtenir les résultats d'intérêt et documentation des analyses (voir 5.2.5).

Étape 5: Représentation et interprétation des résultats des analyses et documentation de cette représentation (voir 5.2.6).

Si les résultats ne sont pas d'une qualité adéquate ou requise, il peut s'avérer nécessaire d'ajouter d'autres (sous-) modèles (revenir à l'Étape 2) ou de préciser des (sous-) modèles existants (revenir à l'Étape 3).

Toutes les étapes individuelles et leurs résultats doivent être documentés en continu.

5.2 Étapes à exécuter en détail

5.2.1 Généralités

Dans ce paragraphe, les étapes sont décrites plus en détail. À chaque étape, le travail ayant été effectué à cette étape doit être documenté.

5.2.2 Description des parties et des fonctions principales du système (Étape 1)

Les concepts suivants du système qui doit être modélisé et analysé doivent être identifiés et décrits comme suit:

a) limites, contexte, et environnement, en particulier associé à la sûreté de fonctionnement et exigences;

b) parties principales (par exemple, installation et équipement de contrôle);

c) fonctions principales (fonctionnement et contrôle/protection) et but.

Cette description peut être effectuée en utilisant du texte libre, des tableaux ou des figures, selon le cas.

5.2.3 Modélisation de la structure du système en se basant sur des sous-modèles de réseau de Petri et leurs relations (Étape 2)

Les systèmes dynamiques, par exemple les systèmes d'automatisation, peuvent généralement être divisés en sous-systèmes «installation non contrôlée» et «contrôle de l'installation». Afin d'empêcher l'installation de passer dans des états non désirés, celle-ci est contrôlée par le contrôle de l'installation. De cette manière, «l'installation non contrôlée» devient «l'installation contrôlée». De plus, chacun de ces sous-systèmes peut être interprété du point de vue fonctionnel et du point de vue de la sûreté de fonctionnement. Par exemple, puisque le contrôle de l'installation ne fonctionne pas toujours correctement, on doit tenir compte de la sûreté de fonctionnement du contrôle – la sûreté de fonctionnement du système dépend de la sûreté de fonctionnement de son contrôle. Puisque le modèle destiné à être développé dépend de la complexité du système et de la tâche d'analyse, le modèle global est constitué généralement d'un sous-ensemble des quatre sous-modèles suivants (il peut se produire par exemple le cas où des résultats adéquats peuvent être obtenus sans modéliser la sûreté de fonctionnement de l'installation), c'est-à-dire un sous-modèle pour spécifier:

a) les fonctions de l'installation;

b) la sûreté de fonctionnement de l'installation;

c) les fonctions du contrôle;

d) la sûreté de fonctionnement du contrôle.

Dans a), le sous-système fonctionnel devant être contrôlé, c'est-à-dire l'installation, doit être modélisé. En l'absence de tout contrôle, ce sous-système dynamique créerait une diversité de processus dans un espace d'état immense, modélisé par le RG de son PN. Certains des états de ce RG doivent être évités car ils représentent des dangers et conduisent à des situations critiques vis-à-vis de la sécurité telles que des impasses, des immobilisations ou d'autres états indisponibles.

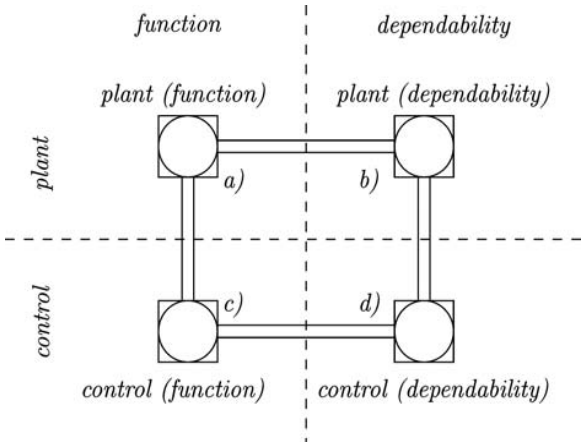
Dans b) la sûreté de fonctionnement de l'installation doit être modélisée. Dans ce sous-modèle, les incertitudes concernant le comportement de l'installation doivent être prises en compte (par exemple, le comportement humain et les influences liées à l'environnement).

Puisque la sûreté de fonctionnement de l'installation influe sur la disponibilité, l'exactitude, la sécurité et d'autres fonctions, les deux sous-modèles a) et b) sont interconnectés.

Dans c), le sous-système servant à contrôler l'installation pour limiter le processus fonctionnel doit être spécifié. Dans ce sous-modèle, la possibilité de défaillances du contrôle n'est pas prise en compte, on suppose que la tâche de contrôle est exécutée parfaitement. Les liaisons appropriées avec les modèles a) et b) conduisent donc à un RG sans aucun état indésirable (par exemple, dangereux ou accidentel).

Dans d) le sous-modèle qui spécifie la réalisation physique du contrôle en particulier vis-à-vis de la sûreté de fonctionnement est modélisé. Ce modèle dépend de la mise en œuvre technique ou des opérateurs humains et des influences liées à l'environnement. Au moyen d'une liaison adéquate avec le sous-modèle de c), les défaillances et comportements incorrects possibles du contrôle sont considérés. Puisqu'ils ont une influence sur les fonctions de contrôle modélisées dans c), dans le modèle global, c'est-à-dire le modèle constitué des sous-modèles (connectés) a) à d), l'installation ainsi que le contrôle et la sûreté de fonctionnement du contrôle sont considérés. De cette manière, le RG correspondant contient des états dangereux et accidentels avec leurs probabilités correspondantes.

En ce qui concerne les différentes couches fonctionnelles et leurs aspects de sûreté de fonctionnement, la sous-structure orthogonale résultante est représentée à la Figure 7.



Légende

Anglais	Français
Function	Fonction
Dependability	Sûreté de fonctionnement
Plant (function)	Installation (fonction)
Plant (dependability)	Installation (sûreté de fonctionnement)
Plant	Installation
Control	Contrôle
Control (function)	Contrôle (fonction)
Control (dependability)	Contrôle (sûreté de fonctionnement)

Figure 7 – Structure de modélisation concernant les deux parties principales «installation» et «contrôle» avec des modèles pour leurs fonctions et la sûreté de fonctionnement

Un modèle intégré de l'ensemble du système peut facilement être déterminé si chacun des différents sous-systèmes est modélisé par un réseau de Petri simple conformément aux paragraphes précédents. Les modèles du réseau de Petri simple sont de préférence reliés par des arcs d'essai et inhibiteurs. Ceci autorise une approche modulaire. Ainsi, un quelconque

sous-système peut être modifié ou changé individuellement sans aucun effet secondaire sur ses modèles voisins.

Dans la documentation de cette étape, les sous-modèles principaux du système ayant été pris en compte et leurs relations doivent être identifiés. Ici, la limite de chaque sous-modèle, leurs parties principales, les fonctions et le but doivent être documentés par des moyens de description classiques, par exemple textuellement, avec des tableaux ou des figures.

S'il n'est pas nécessaire (par exemple pour des systèmes très simples) ou très difficile de diviser un système en ces sous-systèmes, le concepteur du modèle doit en déclarer les raisons clairement et de façon compréhensible.

5.2.4 Précision des modèles de l'Étape 2 jusqu'à atteindre le niveau de détail requis (Étape 3).

Dans cette étape, le modèle ayant été développé à l'Étape 2 doit être précisé et les modèles développés doivent être documentés. Ceci doit être réalisé de manière itérative.

Dans cette étape, un modèle de PN du modèle réalisé à l'Étape 2 doit être précisé. Ceci inclut chacun des sous-systèmes ayant été pris en compte.

Cette précision doit être poursuivie jusqu'à avoir atteint le niveau de détail requis, c'est-à-dire jusqu'à ce que toutes les informations nécessaires pour les analyses à effectuer à l'Étape 4 (voir 5.2.5) soient incorporées:

a) Il est obligatoire que chaque nœud soit étiqueté avec un identifiant unique. Si l'on traite des réseaux synchronisés, le concept de temps doit être clarifié de manière symbolique. Il est recommandé d'utiliser les symboles définis en 3.2.

b) Il est obligatoire de spécifier les autres détails du concept de temps, c'est-à-dire les paramètres spécifiques (par exemple, les poids des transitions causales, les durées fixes, les transitions déterministes, les CDF (fonctions de distribution cumulative) avec les paramètres correspondants des transitions stochastiques, etc.) ainsi que les protections de transition, la politique de mémoire des transitions (les temps d'activation d'une transition sont-ils cumulés ou la transition est-elle sans mémoire? c'est-à-dire la politique de préemption, voir [3]), la capacité des places, etc. Ces informations peuvent être directement incluses dans le réseau si la lisibilité n'est pas affectée. Sinon, on peut choisir une représentation par tableaux ou matrices.

La documentation de cette étape peut être réalisée avec précision par étapes selon la procédure de précision du modèle. La documentation de cette étape doit contenir:

c) Une représentation par PN des sous-systèmes et le cas échéant, du modèle complet.

d) Une description textuelle de chacun des sous-systèmes (au moins pour le niveau modélisé le plus bas).

e) La base pour les paramètres de fiabilité (par exemple, défaillance et rétablissement, hypothèses ou données statistiques) et pour la structure du système.

5.2.5 Analyse du modèle pour obtenir les résultats d'intérêt (Étape 4)

En ce qui concerne les outils, on peut trouver dans [13] certains outils de PN bien connus.

L'approche à choisir pour analyser le modèle au travers de sa nature dépend des résultats d'intérêt. De plus, les méthodes d'analyse applicables (voir Figure 8) sont limitées par le PN sous-jacent et par la disponibilité des informations. On distingue principalement deux alternatives:

a) Des analyses qualitatives, qui répondent à des questions concernant la possibilité, par exemple, d'atteindre un état (global) ou de tirer une certaine séquence de transition de façon répétée.

Les analyses qualitatives sont principalement basées sur le RG non synchronisé. Un RG non synchronisé peut être généré, au moins théoriquement, si, en partant du marquage initial, seul un nombre fini de marquages peuvent être atteints. Dans des conditions spécifiques, il est possible de le déterminer d'après les propriétés du RG non synchronisé concernant la dynamique pour le cas synchronisé ([14]). Si le nombre de marquages pouvant être atteints est trop grand ou même infini, alors il existe d'autres approches: des analyses structurelles, c'est-à-dire des invariants, des impasses et des pièges permettent au moins de tirer des conclusions concernant les mesures de qualité pour le système modélisé ([11] et [14]).

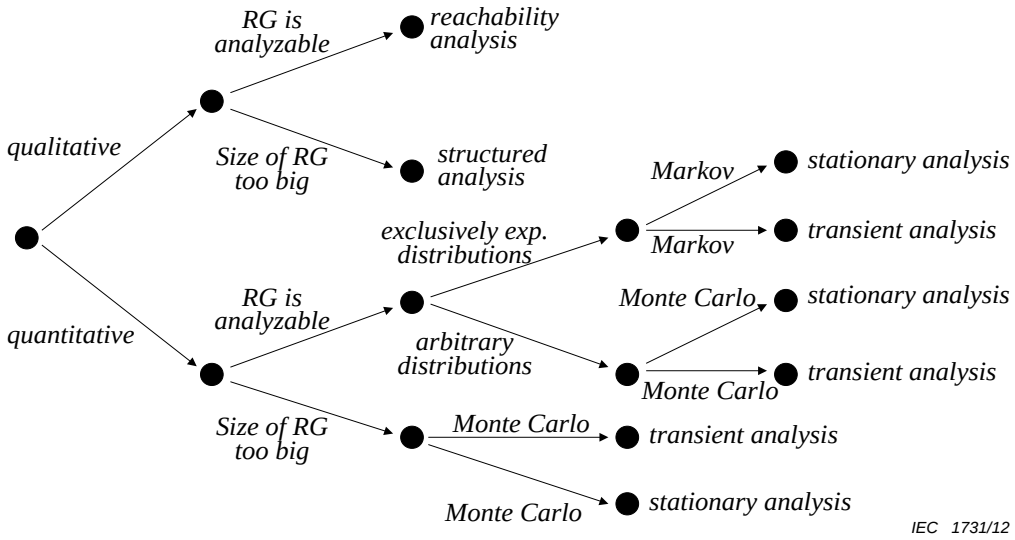
b) Des analyses quantitatives répondent à des questions concernant la probabilité de résultats qualitatifs, par exemple la probabilité d'atteindre un certain état où la probabilité de tirer une certaine transition, des mesures de fiabilité ou de sûreté de fonctionnement, telles que la probabilité de défaillance, le taux de défaillance, le MTTF (Moyenne des temps avant défaillance) ou le MTBF (Temps moyen entre défaillances). Ces concepts peuvent être utilisés comme base pour calculer par exemple la disponibilité de production moyenne.

   Les analyses quantitatives sont principalement basées sur le RG synchronisé ou stochastique. Comme pour le RG non synchronisé, on peut analyser le RG synchronisé si le nombre de marquages pouvant être atteints n'est pas trop grand. En fonction des transitions se trouvant dans le PN, il existe deux alternatives:

   i) si toutes les transitions dans le PN synchronisé ont une durée de tir distribuée de manière exponentielle sur une période définie de temps d'intérêt (c'est-à-dire qu'elles ont un taux de tir constant sur une période définie de temps), on peut transformer le RG synchronisé en une chaîne de Markov et effectuer l'analyse stationnaire ou transitoire;

   ii) sinon, on doit utiliser l'approche de la simulation de Monte-Carlo et effectuer une analyse stationnaire ou transitoire.

Si le nombre de marquages pouvant être atteints est trop grand, on doit utiliser l'approche de Monte-Carlo et également effectuer des analyses transitoires. Le nombre d'états pouvant être gérés dépend des propriétés logicielles et matérielles. De nos jours, des systèmes ayant environ 10^8 états restent encore gérables. Les systèmes ayant plusieurs millions d'états peuvent correspondre à des «petits» systèmes.



Légende

Anglais	Français
Anglais	Français
RG is analysable	RG est analysable
Reachability analysis	Analyse d'atteignabilité
Qualitative	Qualitative
Size of RG too big	RG est de trop grande taille
Structured analysis	Analyse structurée
Markov	Markov
Stationary analysis	Analyse stationnaire
Quantitative	Quantitative
RG is analysable	RG est analysable
Exclusively exponential distributions	Distributions exponentielles exclusivement
Markov	Markov
Transient analysis	Analyse transitoire
Markov	Markov
Transient analysis	Analyse transitoire
Arbitrary distributions	Distributions arbitraires
Monte Carlo	Monte-Carlo
Stationary analysis	Analyse stationnaire
Monte Carlo	Monte-Carlo
Stationary analysis	Analyse stationnaire
Size of RG too big	RG est de trop grande taille
Monte Carlo	Monte-Carlo
Transient analysis	Analyse transitoire
Monte Carlo	Monte-Carlo
Stationary analysis	Analyse stationnaire

Figure 8 – Indication de la méthode d'analyse en fonction du modèle de PN

La documentation de cette étape doit contenir:

c) les méthodes choisies pour calculer les résultats d'intérêt, qui doivent être énumérées;

d) les outils ayant été appliqués pour effectuer les calculs, l'équipement de calcul et les conditions des données et les réglages par défaut, qui doivent être énumérés.

5.2.6 Représentation et interprétation des résultats des analyses (Étape 5)

La sortie de cet état doit satisfaire aux exigences suivantes:

a) le RG doit être représenté de manière adéquate. En général, le concept d'états agrégés sera nécessaire car le RG est trop grand si chacun des états est énuméré;

b) l'influence de différentes valeurs de paramètres ou structures de système doit être représentée de manière adéquate: par exemple, l'influence de différents paramètres de maintenabilité et de fiabilité ainsi que différentes structures de système (par exemple, des aménagements de redondance) sur la disponibilité et la sécurité peut être représentée sur un diagramme qui indique la disponibilité du système en fonction de sa sécurité.

Les résultats d'une analyse doivent être interprétés textuellement d'une façon claire et concrète. De plus, il convient que les résultats d'analyse indiquent d'autres réalisations (concernant la structure du système ou la mise en œuvre des sous-modèles).

5.2.7 Résumé de la documentation (Étape 6)

La documentation correspond généralement aux exigences de gestion de la qualité. Dans certains domaines, en particulier les applications critiques du point de vue de la sécurité, une documentation spécifique est obligatoire, par exemple dans les installations ferroviaires, l'aviation ou dans les centrales nucléaires, voir Tableau 5.

Tableau 5 – Parties obligatoires et recommandées de la documentation

N°	Étape	Représentation des méthodes et moyens		
		Obligatoire	**Fortement recommandée**	**Recommandée**
1	Documentation générale: description générale du système, fonction, parties et limites; objectif et domaine d'application de l'analyse; justification de la raison de l'utilisation des techniques des réseaux de Petri.	 Texte et figures Texte Texte		
2	Documentation de quatre sous-modèles (voir 5.2.3)	Texte et figures	PN de haut niveau	
3	Documentation détaillée: modèles de précision du système (couches d'abstraction); source de données utilisées (hypothèses ou données statistiques ?) pour les taux de pannes et de rétablissement	 Texte et figures Texte	Tableaux	 b) Tableaux
4	Méthodes d'analyse: description des méthodes; description de l'ordinateur et des outils utilisés	 Texte Texte		 a) Tableaux b) Tableaux
5	Résultats: sous forme numérique et graphique; Interprétation des résultats	 Texte et figures Texte		 a) Tableaux

6 Relation avec les autres modèles de sûreté de fonctionnement

Parfois, seule la chaîne cause-conséquence d'un quelconque événement ponctuel, par exemple une défaillance du système, est d'intérêt ou inversement, les raisons d'un défaut du système, à savoir un état global au moyen d'un événement ou d'un état de base, sont d'intérêt. Ces analyses résultent des techniques d'analyse AAP (Analyse par arbre de panne), AAE (Analyse par arbre d'événement), BDF (Bloc-diagramme de fiabilité) ou AMDE (Analyse des modes de défaillance et de leurs effets). Le graphe d'atteignabilité comporte toutes ces informations. Ainsi, ces relations de cause à effet peuvent être déterminées d'après le RG et représentées de la manière classique ([10]).

Ceci résulte du fait que la puissance de la modélisation des PN est plus grande que celle des AAP, AAE et BDF. On peut montrer ainsi que ces modèles peuvent être transformés en réseaux de Petri sans perte d'information [15]. Puisque les chaînes de Markov supposent des taux de transition constants impliquant exclusivement des durées d'état distribuées de manière exponentielle, les PN stochastiques généraux ont une plus grande puissance de modélisation. Les informations obtenues en exécutant une AMDE ou une AMDE(C) peuvent être utilisées pour construire le modèle de PN du système. Bien qu'en particulier l'AMDE(C) puisse fournir un processus formel avec des procédures et des formes spécifiées, elles ne sont pas formelles au sens mathématique. De plus, elles ne permettent d'analyser que des défaillances simples et en conséquence, il convient qu'elles ne fournissent pas des «modèles» des systèmes globaux (sauf pour le cas très simple des systèmes série). Cependant, lorsqu'elles sont utilisées en complément des PN, elles peuvent être très efficaces comme base pour rassembler des informations concernant le système.

Annexe A
(informative)

Structure et dynamique des réseaux de Petri

A.1 Concept général d'un réseau de Petri et sa relation avec la fiabilité

A.1.1 Remarques introductives

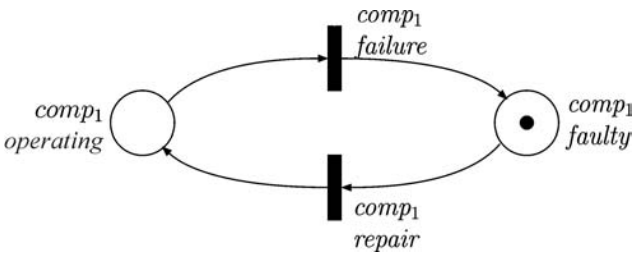
La vue d'ensemble des réseaux de Petri peut être caractérisée et la sûreté de fonctionnement interprétée comme suit: les éléments actifs et passifs sont différenciés (voir Tableau 1). Les éléments passifs sont appelés «places»; ils modélisent des conditions, par exemple, des états élémentaires distinctifs avec une certaine durée. Les transitions représentent les éléments actifs (par exemple, des événements ou des règles logiques) qui modifient les états élémentaires en se basant sur la règle de tir.

Les transitions sont «activées» lorsque les conditions nécessaires sont satisfaites, c'est-à-dire lorsque les places correspondantes portent un certain nombre de jetons. En commutant une transition, c'est-à-dire l'événement, de nouvelles conditions peuvent devenir valides et les conditions préalables peuvent perdre leur validité.

A.1.2 Structure d'un réseau de Petri

Puisque les réseaux de Petri sont des graphes «biparti», chaque arc est relié à deux types de nœud différents. Ceci signifie, qu'entre deux états qui se suivent (par exemple défectueux et fonctionnel), il doit y avoir un événement conduisant d'un état à l'autre (par exemple, une réparation). D'autre part, entre deux événements quelconques qui se suivent (par exemple, une défaillance et une réparation), il existe un état intermédiaire atteint (par exemple, défectueux) – voir Figure A.1 (ici et dans les figures qui suivent, «$comp_1$ faulty» est une abréviation de «$component_1$ faulty and under repair» ($composant_1$ défectueux et en cours de réparation). Les relations entre les états et les événements sont représentés par des arcs dirigés. Le «pré-ensemble» d'un nœud n est l'ensemble de tous les nœuds n_1 avec un arc dirigé de n_1 à n. Le «post-ensemble» de n est l'ensemble de tous les nœuds n_2 avec un arc dirigé de n à n_2. Hormis «pré-ensemble» et «post-ensemble», on se réfère souvent à ces ensembles par les places «amont» et «aval».

Il convient que les PN modélisent tous les états pertinents pouvant être pris et toutes les relations cause-conséquence possibles pouvant survenir, en fonction des conditions, c'est-à-dire un ensemble d'états.



IEC 1732/12

Légende

Anglais	Français
$Comp_1$ failure	$Comp_1$ défaillance
$Comp_1$ operating	$Comp_1$ fonctionnel
$Comp_1$ faulty	$Comp_1$ défectueux
$Comp_1$ repair	$Comp_1$ réparation

Figure A.1 – Cercle de disponibilité état-transition d'un composant

A.1.3 Dynamique causale dans les réseaux de Petri de bas niveau

A.1.3.1 Généralités

Dans les PN, un exemple de la dynamique des systèmes peut être la visualisation des états et des transitions d'états du système par rapport à leurs relations.

A.1.3.2 Marquage

Les places peuvent être marquées avec des jetons («points noirs») qui représentent l'occurrence réelle d'un état local ou «marquage local». L'ensemble de tous les marquages locaux est appelé «marquage du réseau» ou «marquage global». Le marquage du réseau avant le tir de l'une quelconque de ses transitions est appelé «marquage initial».

Le marquage des places peut être modifié par la «commutation» ou le «tir» des transitions. Ceci conduit à la dynamique des réseaux qui peut être illustrée par le «flux de jetons».

A.1.3.3 Flux de jetons et règle de tir

Une transition est activée (c'est-à-dire qu'elle peut «tirer») si toutes les places dans son pré-ensemble sont marquées avec un nombre approprié de jetons. Une transition effectuant un tir peut éliminer les jetons des places du pré-ensemble (correspondant aux types et aux poids des arcs reliant ses places de pré-ensemble) et produit des jetons sur ses places de post-ensemble (voir Figure A.2 et Figure A.3). Ceci signifie que des jetons sont réellement absorbés (ou détruits) et produits, seule la simulation du comportement du réseau les fait ressembler à un flux. En général, la survenance d'un événement local modifie les états locaux à son voisinage direct. Ceci peut être interprété comme suit: si un événement survient (par exemple, si une défaillance survient) l'état du système est modifié (ici de «fonctionnel» à «défectueux»). De plus, les transitions peuvent être pondérées en fonction de la probabilité de leur occurrence: dans un état avec plusieurs transitions activées, la transition ayant le poids le plus élevé tire avec la probabilité la plus forte ([3]).

En relation avec la sûreté de fonctionnement, l'occurrence d'une défaillance modifie l'état du système de «fonctionnel» à «défectueux» et la condition «contrainte excessive» n'est plus vérifiée.

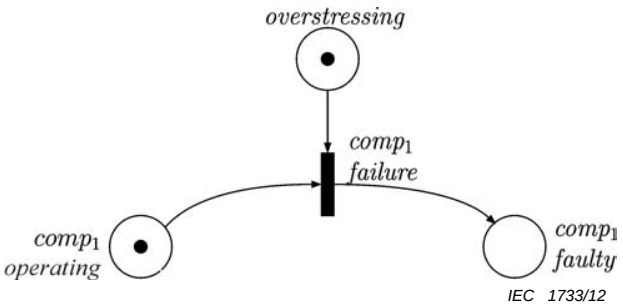


Figure A.2 – La transition «défaillance» est activée

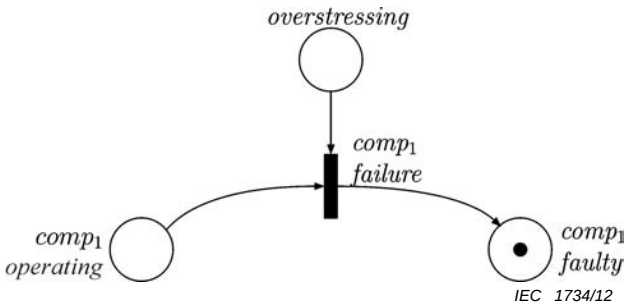


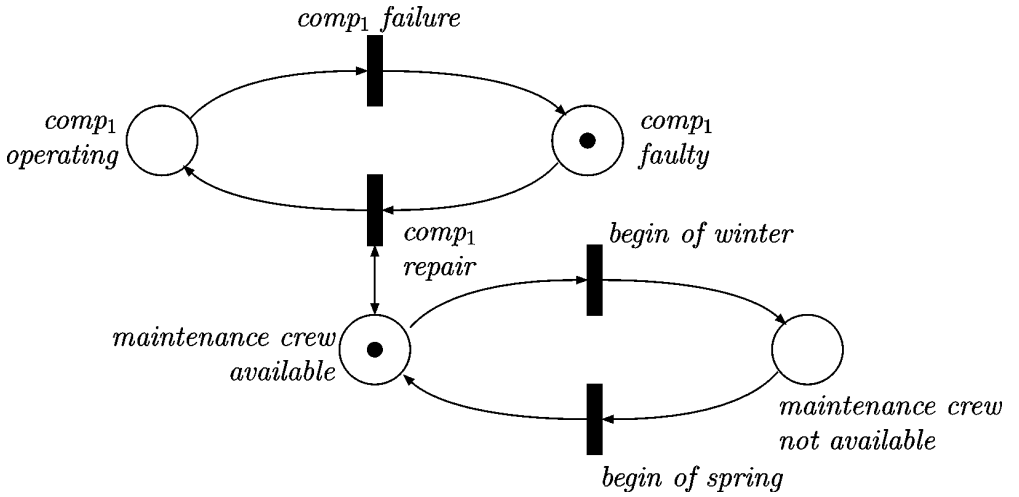
Figure A.3 – La place «défectueux» est marquée en raison du tir de «défaillance»

Légende

Anglais	Français
Overstressing	Contrainte excessive
$Comp_1$ operating	$Comp_1$ fonctionnel
$Comp_1$ failure	$Comp_1$ défaillance
$Comp_1$ faulty	$Comp_1$ défectueux

A.1.3.4 Arcs d'essai

Les transitions qui sont reliées à une place par un «arc d'essai» ou un «arc de communication» ne modifient pas le nombre de jetons à cette place. De cette manière, elles permettent de lire si une place est marquée ou non. Les arcs d'essai sont dessinés sous forme de flèches doubles (par exemple, entre «maintenance crew» (équipe de maintenance) et «repair» (réparation) sur les Figures A.4 et A.5). Ils empêchent ici une réparation de survenir en hiver (l'équipe de maintenance n'est pas disponible). Il convient de noter que cet exemple est fortement simplifié afin de se concentrer sur la signification des arcs d'essai.



Légende pour les Figures A.4 et A.5

Anglais	Français
$Comp_1$ failure	$Comp_1$ défaillance
$Comp_1$ operating	$Comp_1$ fonctionnel
$Comp_1$ faulty	$Comp_1$ défectueux
$Comp_1$ repair	$Comp_1$ réparation
Beginning of winter	Au début de 'hiver
Maintenance crew available	Equipe de maintenance disponible
Maintentance crew not available	Equipe de maintenance n'est pas disponible
Beginning of spring	Au début du printemps

Figure A.4 – La transition «$comp_1$ réparation»est activée

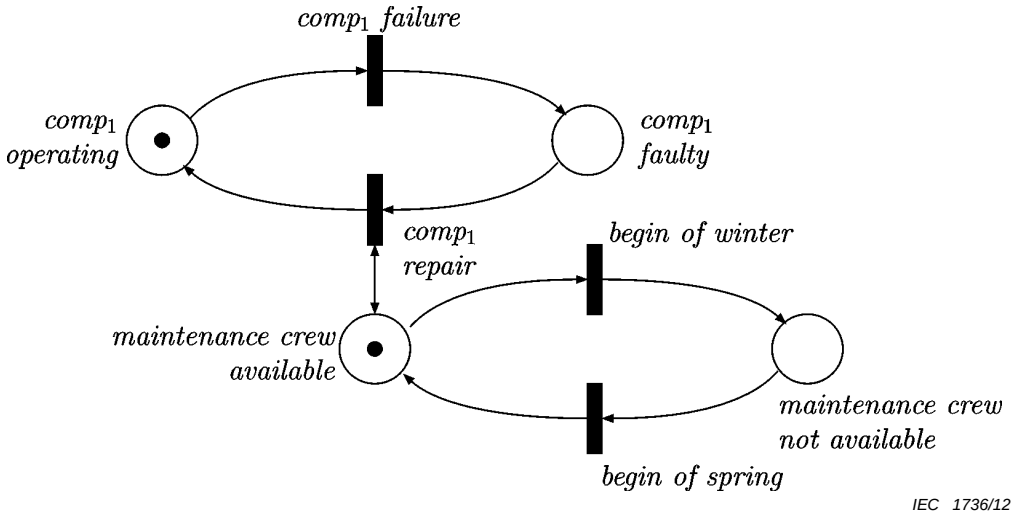
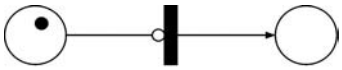


Figure A.5 – Le jeton à la place «maintenance crew available» (équipe de maintenance disponible) n'est pas consommé

Sur la Figure A.4, la transition «repair» (réparation) vérifie s'il y a une «maintenance crew» (équipe de maintenance) disponible, c'est-à-dire au moins un jeton à cette place. Dans ce cas, l'essai est réussi. La transition est activée et le tir conduit au marquage représenté sur le réseau de la Figure A.5.

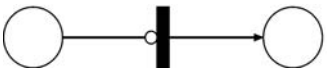
A.1.3.5 Arcs inhibiteurs

Les transitions qui sont reliées par l'intermédiaire d'arcs inhibiteurs avec leurs places de pré-ensemble ne sont activées que si le nombre de jetons à ces places est strictement inférieur au poids des arcs inhibiteurs correspondants. C'est-à-dire que, lorsque les poids sont égaux à un, ils ne sont activés que si les places ne portent aucun jeton. Les arcs inhibiteurs sont dessinés avec un petit cercle au lieu d'une pointe de flèche. Le tir d'une telle transition ne modifie pas le marquage sur les places de pré-ensemble correspondantes.



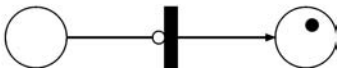
IEC 1737/12

Figure A.6 – La transition n'est pas activée



IEC 1738/12

Figure A.7 – Marquage avant tir



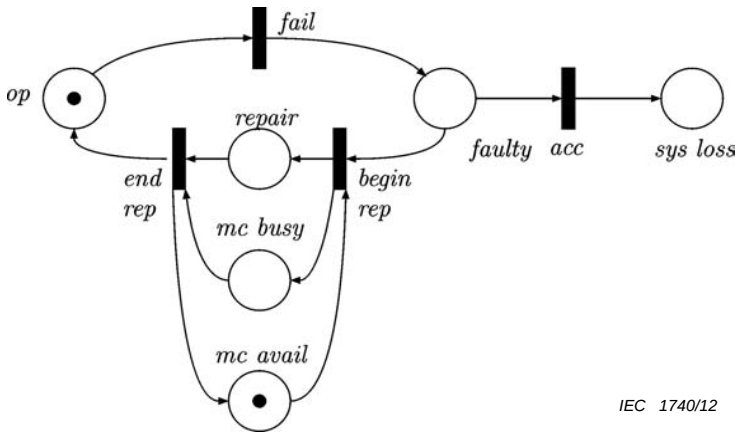
IEC 1739/12

Figure A.8 – Marquage après tir

Puisque la transition des réseaux de la Figure A.6, la Figure A.7 et la Figure A.8 n'est activée que si la place dans son pré-ensemble n'est pas marquée, la transition dans le réseau de la Figure A.6 n'est pas activée. Dans le réseau de la Figure A.7, la transition est activée et le tir conduit au marquage représenté sur le réseau de la Figure A.8. Il convient de noter que sur la Figure A.8, la transition peut être tirée de manière extrêmement fréquente; on peut l'empêcher par un deuxième arc inhibiteur conduisant de la place dans le post-ensemble de la transition jusqu'à la transition. Tout comme des arcs ordinaires, les arcs inhibiteurs peuvent être pondérés (voir 4.4). On peut trouver un exemple d'application d'arc inhibiteur en A.1.3.

A.1.4 Graphe d'atteignabilité

Le graphe d'atteignabilité (RG) d'un PN représente tous les marquages globaux pouvant être atteints en raison du tir de transitions en commençant par un «marquage initial» donné. Le RG représente ainsi le comportement possible d'un système en décrivant explicitement son espace d'état.



IEC 1740/12

Légende pour les Figures A.9 et A.10

Anglais	Français
Fail / Operating / Repair / End repair / Begin repair / Faulty / Accident / System loss / Maintenance crew busy / Maintenance crew available	Echec / Fonctionnel / Réparation / Début de réparation / Fin de réparation / Défectueux / Accident / Perte système / Equipe de maintenance occupée / Equipe de maintenance disponible

Figure A.9 – PN avec marquage initial

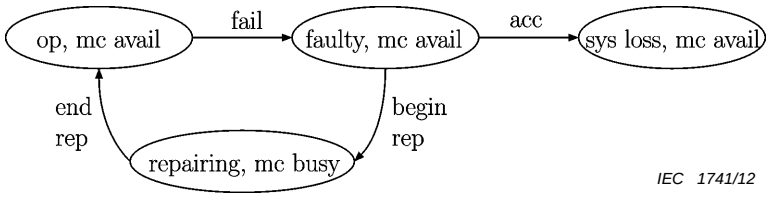


Figure A.10 – RG correspondant

L'espace des états atteignables du réseau de Petri sur la Figure A.9 est constitué de quatre états globaux (voir Figure A.10). Il convient de noter que cet exemple est fortement simplifié afin de se concentrer sur la signification des arcs d'atteignabilité.

Chaque état global est dessiné par un cercle ou une ellipse qui est identifié de façon définie par le marquage réel du réseau. En raison de ses annotations d'arc, le RG spécifie la façon dont le changement d'un état global à un autre est effectué. Pour des réseaux de Petri plus complexes, le nombre d'états globaux dans le RG peut augmenter rapidement avec le nombre de composants. La construction de son RG peut être effectuée automatiquement par des outils informatiques.

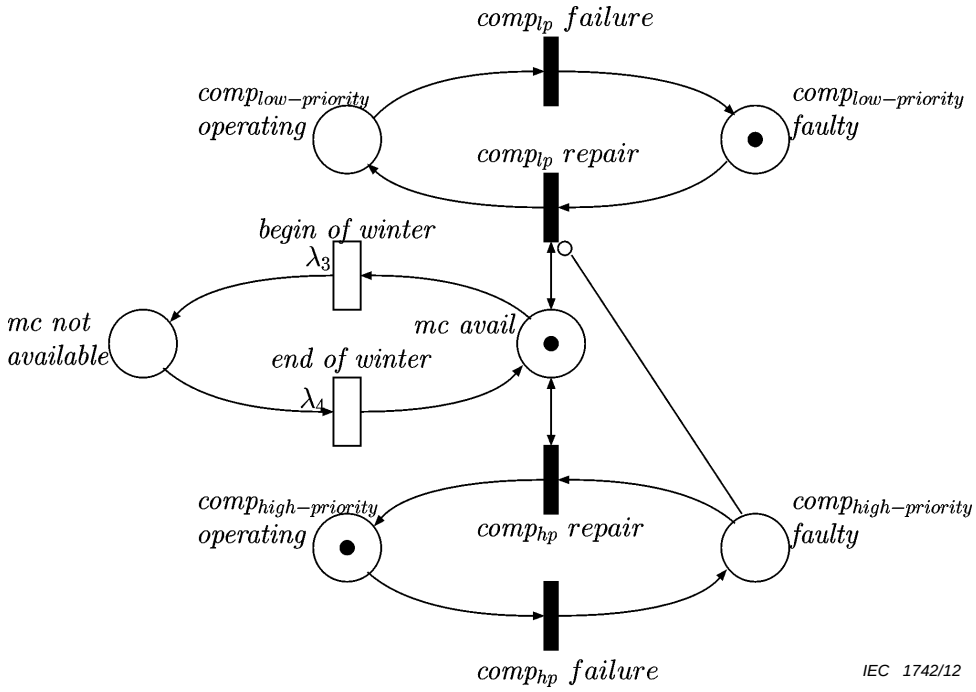
Le Tableau A.1 donne une vue d'ensemble des concepts correspondants entre les systèmes en général, le réseau de Petri, les graphes d'atteignabilité et le concept de sûreté de fonctionnement.

Tableau A.1 – Concepts correspondants dans les systèmes, réseaux de Petri et graphes d'atteignabilité ainsi que sûreté de fonctionnement

Aspect	Système	Réseau de Petri	Graphe d'atteignabilité	Sûreté de fonctionnement
Dynamique	Événement	Transition	Arc	Par exemple: Événements de défaut ou événements de traitement d'erreur
Statique	État local	Place		État local
	État global	Marquage = ensemble de places marquées	Nœud	État global (par exemple, maintenance, danger)
	État global agrégé	Ensemble de marquages	Ensemble de nœuds	Ensemble d'états globaux (par exemple, disponible, sûr)

Exemple

Dans le réseau de Petri de la Figure A.11 la transition «$comp_{pb}$ réparation» (abréviation de «$composant_{priorité\ basse}$réparation») est activée, car la place «$comp_{priorité\ basse}$ défectueux» est marquée, les équipes de maintenance sont disponibles (au moins une équipe est nécessaire pour réparer ce composant) et «$comp_{priorité\ haute}$» n'est pas défectueux. De plus, la transition «$comp_{ph}$ échec» (abréviation de «$component_{priorité\ haute}$ échec») est activée en raison de la satisfaction de la condition «$comp_{priorité\ haute}$ operationnel».



Légende pour les Figures A.11 et A.12

Anglais	Français
Anglais	Français
$Comp_{lp}$ failure / $Comp_{low-priority}$ operating / $Comp_{lp}$ repair / $Comp_{low-priority}$ faulty / Begin of winter / Maintenance crew not available / End of winter / Maintenance crew available / $Comp_{high-priority}$ operating / $Comp_{hp}$ repair / $Comp_{high-priority}$ faulty / $Comp_{hp}$ failure	$Comp_{pb}$ échec / $Comp_{priorité\ basse}$ fonctonnel / $Comp_{pb}$ réparation / $Comp_{priorité\ basse}$ défectueux / Début de l'hiver / Equipe de maintenance occupée / Fin d'hiver / Equipe de maintenance disponible / $Comp_{priorité\ haute}$ fonctonnel / $Comp_{ph}$ réparation / $Comp_{priorité\ haute}$ défectueux / $Comp_{ph}$ échec

Figure A.11 – Les transitions '$comp_{pb}$ réparation' et '$comp_{ph}$ échec' sont activées

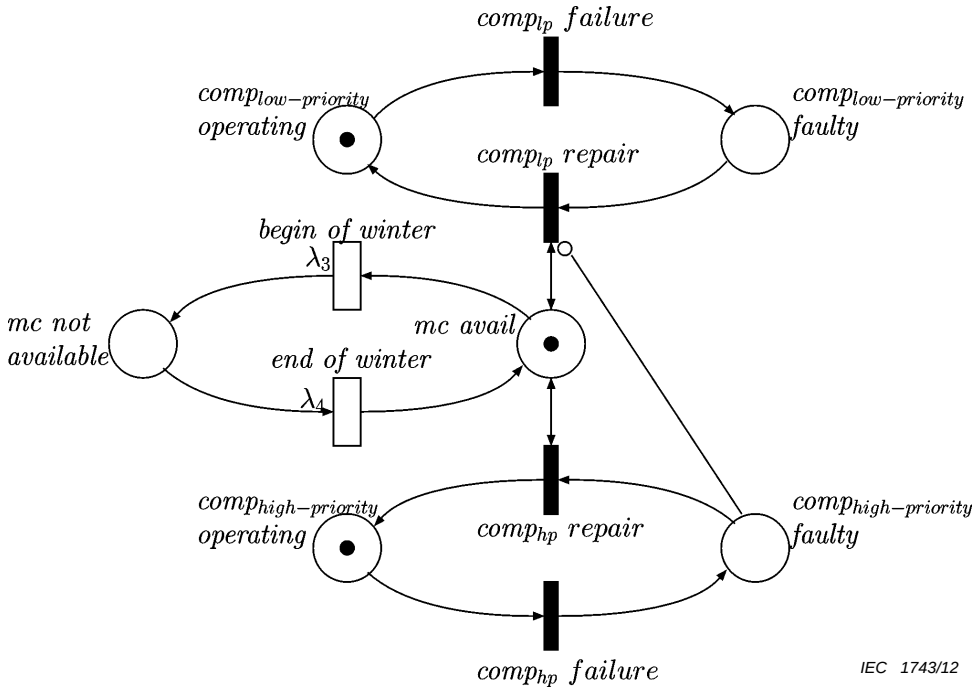


Figure A.12 – Marquage après tir de la transition «$comp_{pb}$ réparation»

Le tir de «comp$_{pb}$ réparation» absorbe un jeton depuis la place «comp$_{priorité\ basse}$ faulty» et produit un jeton à la place «comp$_{priorité\text{-}basse}$ operating». Puisque les places «comp$_{priorité\text{-}haute}$ défectueux» et «équipe de maintentance disponible» sont respectivement reliées à la transition «comp$_{lp}$ réparation» par des arcs d'essai et inhibiteur, leur marquage n'est pas modifié (voir Figure A.12).

Noter le comportement du réseau dans un autre état: si le composant ayant la priorité haute présente une défaillance tandis que le composant avec la priorité basse est en cours de réparation, alors

a) la réparation du composant de priorité basse est interrompue,

b) la réparation du composant de priorité haute démarre,

c) la réparation du composant de priorité basse redémarre après la fin de la réparation du composant de priorité haute.

La modélisation de ces événements «interrompus» par des calculs analytiques est très difficile, tandis que la simulation de Monte-Carlo permet d'analyser très facilement ces modèles.

A.2 Réseaux de Petri synchronisés

A.2.1 Remarques introductives

Pour les applications à la sûreté de fonctionnement, il est également utile de modéliser les aspects temporels. Par exemple, le moment où un système est activé ou désactivé est représenté par le moment où le réseau se trouve dans le marquage correspondant. D'autre part, les retards après lesquels les états changent sont attribués aux transitions. En considérant le temps, on peut distinguer le comportement déterministe et le comportement stochastique. Ces deux catégories peuvent être représentées par des réseaux de Petri synchronisés avec des paramètres temporels déterministes (par exemple, des durées d'événements déterministes) et des paramètres synchronisés stochastiques (par exemple, des fonctions exponentielles avec des taux correspondants) sur leurs transitions (pour les PN synchronisés stochastiques, voir [3] et [16]). Dans tous les cas, les propriétés des transitions sont représentées par diverses étiquettes ou conditions supplémentaires.

A.2.2 Transitions spécifiques pour les réseaux de Petri de bas niveau synchronisés

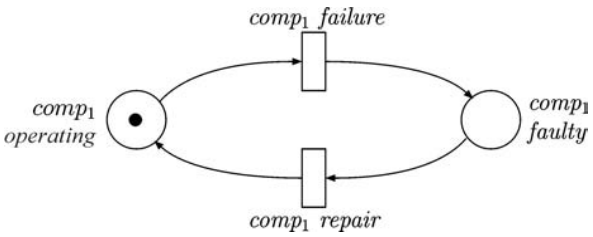
Dans les PN synchronisés, aussi bien des transitions non synchronisées que des transitions synchronisées peuvent être utilisées. En principe, pour les transitions synchronisées, la même règle de tir est valable que celle pour les transitions non synchronisées (voir le PN non synchronisé mentionné ci-dessus). Une transition synchronisée doit être activée pendant une durée spécifique. Cette durée peut être déterministe ou stochastique, selon la fonction de distribution spécifique de transition (CDF) et les paramètres correspondants. À l'expiration de cette durée, la transition est autorisée à tirer. Le Tableau 2 représente les transitions couramment utilisées dans les PN synchronisés.

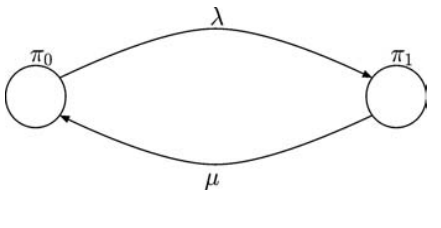
En correspondance avec le type spécifique de transition synchronisée, elle est attribuée par un paramètre temporel qui spécifie la durée de tir déterministe, le taux de tir (constant) ou la distribution de probabilité avec ses paramètres.

Noter que l'utilisation de la distribution de Dirac $\delta(d)$ pour les retards déterministes d permet d'englober à la fois les transitions déterministes et stochastiques dans le même cadre ($\delta(0)$ permet d'englober des transitions non synchronisées et synchronisées). Il est néanmoins souvent utile de distinguer les divers types de comportement car ils correspondent à des événements de nature différente.

A.2.3 Dynamique dans les réseaux de Petri de bas niveau synchronisés

Dans les réseaux de Petri synchronisés, la dynamique du système est également modélisée par la variation de l'avancement des marquages, qui est représentée par son graphe d'atteignabilité correspondant (voir par exemple Figure A.10). En fonction des différents taux de transition ou des distributions stochastiques, leurs arcs de transition d'état sont marqués par leur symbole de temps spécifique. A chaque état global qui modélise un certain état associé à la sûreté de fonctionnement est attribué une certaine probabilité qui résulte du comportement temporel de la transition, par exemple de son tir stochastique. Il a été démontré que tout PN stochastique fini et marqué est isomorphe pour une chaîne de Markov d'espace discret [17] à condition que tous les événements soient distribués de façon exponentielle.





Légende pour les Figures A.13 et A.14

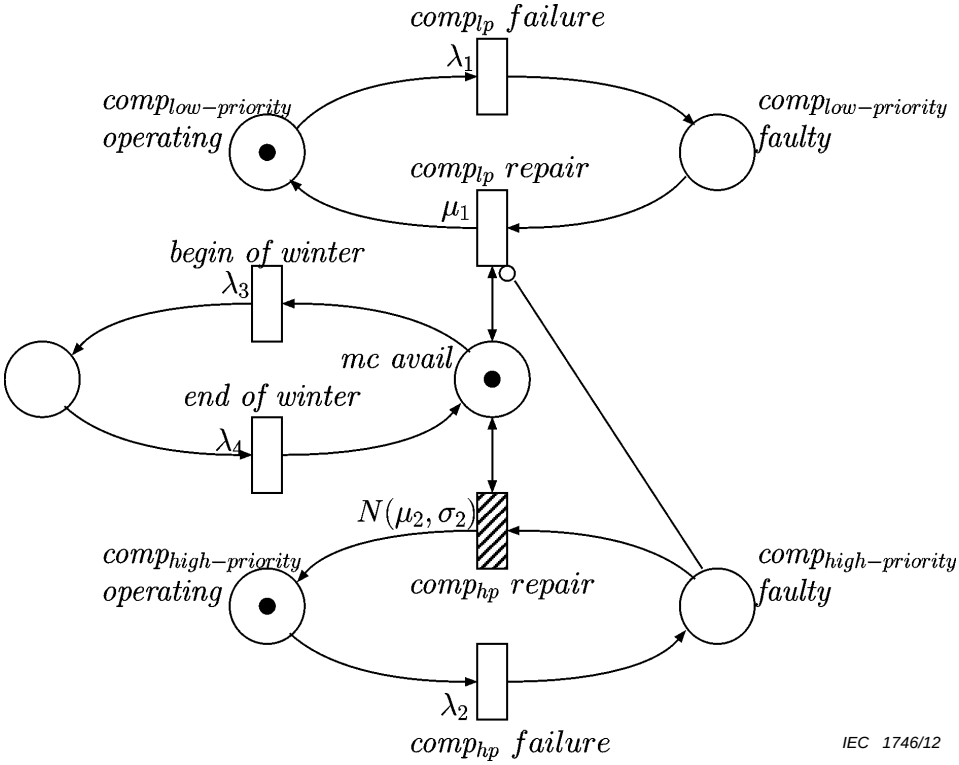
Anglais	Français
$Comp_1$ failure / $Comp_1$ operating / $Comp_1$ faulty / $Comp_1$ repair	$Comp_1$ échec / $Comp_1$ fonctionnel / $Comp_1$ défectueux / $Comp_1$ réparation

Figure A.13 – PN synchronisé avec deux transitions synchronisées distribuées de façon exponentielle

Figure A.14 – Graphe d'atteignabilité stochastique correspondant

Sur la Figure A.13, les transitions sont attribuées avec leurs taux de transition. Sur la Figure A.14, les états globaux sont respectivement nommés π_0 et π_1.

Exemple



Légende

Anglais	Français
$Comp_{lp}$ failure / $Comp_{low\text{-}priority}$ operating / $Comp_{lp}$ repair / $Comp_{low\text{-}priority}$ faulty / Beginning of winter / Maintenance crew available / End of winter / $Comp_{high\text{-}priority}$ operating / $Comp_{hp}$ repair / $Comp_{high\text{-}priority}$ faulty / $Comp_{hp}$ failure	$Comp_{pb}$ échec / $Comp_{priorité\ basse}$ fonctionnel / $Comp_{pb}$ réparation / $Comp_{priorité\ basse}$ défectueux / Début de l'hiver / Fin d'hiver / Equipe de maintenance disponible / $Comp_{priorité\ haute}$ fonctionnel / $Comp_{ph}$ réparation / $Comp_{prioté\ haute}$ défectueux / $Comp_{ph}$ échec

Figure A.15 – Réseau de Petri avec transitions synchronisées

Sur la Figure A.15, la transition «$comp_{pb}$ échec» tire avec un taux λ_1, c'est-à-dire que, lorsque ce composant est dans son état fonctionnel (indiqué par $comp_{priorité\ basse}$ fonctionnel), il y reste pendant une durée distribuée de façon exponentielle. Si $comp_{ph}$ est dans son état défectueux, il y reste pendant un temps distribué de façon normale, spécifié avec le paramètre μ_2 (moyenne) et σ_2 (écart type). Il convient de noter qu'on suppose ici la loi normale tronquée avec un support limité (0,∞) pour la transition $N(\mu_2, \sigma_2)$. De plus, la même remarque s'applique aux événements interrompus comme pour les réseaux des Figures A.11 et A.12.

A.2.4 Classes différentes de réseaux de Petri synchronisés

Il existe un grand nombre de sous-classes de PN stochastiques (SPN). Dans une première classification, on peut déclarer que la classe dépend des choix des distributions de temps de tir ayant une influence significative sur les analyses possibles.

Les classes de modèles suivantes sont courantes dans la documentation (par exemple, [3]):

- réseaux de Petri stochastiques généralisés (GSPN) (*en anglais: generalized stochastic Petri nets*: toutes les transitions synchronisées ont un temps de tir distribué de façon exponentielle;

- SPN markoviens (MSPN): SPN pour lesquels le processus stochastique sous-jacent est une chaîne de Markov. Tel est le cas si toutes les transitions synchronisées ont un temps de tir distribué de façon exponentielle ou si toutes les transitions synchronisées ont un temps de tir distribué de façon géométrique (c'est-à-dire, sans mémoire et à temps discret). La première possibilité correspond aux GSPN;
- réseaux de Petri déterministes et stochastiques (DSPN): les transitions synchronisées sont, soit exponentielles, soit déterministes, et les transitions déterministes sont mutuellement exclusives et ont une politique de préemption particulière;
- réseaux de Petri stochastiques régénérateurs de Markov (MRSPN): SPN pour lesquels le processus stochastique sous-jacent est un processus régénérateur de Markov. Une sous-classe, appelée également DSPN, est fournie par les SPN lorsque les transitions synchronisées sont, soit exponentielles, soit générales, et les transitions générales sont mutuellement exclusives et ont une politique de préemption particulière.
- réseaux de Petri stochastiques non markoviens: tout SPN qui n'est pas markovien.

A.3 Méthodes d'analyse des réseaux de Petri

A.3.1 Généralités

Il existe en général deux tâches d'analyse fondamentalement différentes:

a) des tâches qualitatives qui traitent des questions concernant des possibilités telles que «Est-il possible d'atteindre un certain état ?» ou «Est-il possible qu'un certain événement ait lieu ?»;

b) des tâches quantitatives qui traitent des questions concernant (entre autres) les probabilités, telles que «Quelle est la probabilité d'atteindre un certain état ?» ou «Quelle est la probabilité pour qu'un certain événement ait lieu ?».

En conséquence, les tâches d'analyse peuvent être divisées en tâches qualitatives et quantitatives.

A.3.2 Analyse qualitative

Les analyses qualitatives peuvent être divisées en analyses structurelles et dynamiques:

- les analyses structurelles ne tiennent compte que de la structure du réseau de Petri, elles ne tiennent pas compte du RG. Ces analyses sont donc indépendantes du marquage initial. L'avantage de ces analyses est que les résultats sont valables pour tout marquage initial arbitraire. L'inconvénient est que ces résultats sont souvent relativement généraux. Les invariants, les impasses et les pièges sont des propriétés structurelles bien connues des réseaux de Petri [16];
- les analyses dynamiques tiennent compte du RG ou d'un sous-ensemble de celui-ci, par exemple une séquence (la plus courte) ou un ensemble de séquences d'un réseau de Petri. Puisque le RG est basé sur un marquage initial spécifique, ces résultats dépendent également du marquage initial. L'avantage de ces analyses est que si le RG peut être généré et traité, on peut apporter une réponse à toutes les questions qualitatives. L'inconvénient est qu'il est souvent impossible de créer le RG en raison de sa taille. Les analyses dynamiques identifient par exemple si des états dangereux ou accidentels peuvent survenir [18].

A.3.3 Analyse quantitative

A.3.3.1 Généralités

Souvent, les caractéristiques de sûreté de fonctionnement d'un système et leurs mesures, par exemple la probabilité en régime établi ou transitoire de manœuvrabilité du système, deviennent le centre d'intérêt. Un grand nombre des méthodes et des algorithmes nécessaires pour analyser quantitativement des systèmes trouvent leur fondement dans la théorie des probabilités. On doit naturellement spécifier les distributions de probabilité

appropriées avant de pouvoir effectuer les analyses. S'il n'y a que des distributions exponentielles dans le modèle du système, il s'agit d'un modèle «markovien homogène». Pour résoudre des modèles de ce type, toutes les approches concernant les analyses de chaînes de Markov peuvent être utilisées. La façon d'analyser des modèles à une échelle industrielle est décrite par exemple dans [12]. De plus, les PN se sont révélés très efficace pour les calculs de sécurité des systèmes associés à la sécurité (calcul de SIL) tels que la probabilité de défaillance à la demande (c'est-à-dire l'indisponibilité moyenne) et la probabilité de défaillance par heure (c'est-à-dire la fréquence moyenne de défaillance).

A.3.3.2 Analyse de modèles markoviens

Pour utiliser les méthodes d'analyse pour les CTMC (chaîne de Markov à temps continu, *en anglais: continuous time Markov chain*), un réseau de Petri stochastique est mappé sur une CTMC; pour effectuer ce mappage, il est nécessaire que le PN stochastique soit un GSPN (voir A.2.4, [3]). Deux types de solutions aux processus de Markov ([19]) sont d'intérêt: transitoire et en régime établi. La solution transitoire est obtenue en résolvant «l'équation différentielle de Kolmogorov» et la solution en régime établi est obtenue en résolvant un système d'équations linéaires. Des résultats analytiques sous forme fermée sont possibles soit pour des graphes de Markov fortement structurés, soit pour des très petits graphes de Markov. Dans la plupart des autres cas, on doit recourir à des techniques de solutions numériques.

Les processus de Markov peuvent être utilisés pour évaluer

- la probabilité des états (dépendant du temps et asymptotiques),
- le temps cumulé passé dans les états (par exemple, à des fins de disponibilité de production).

Dans le domaine spécifique des problèmes de disponibilité de production, on utilise des processus de Markov «multi-états», lorsqu'on traite des systèmes de sécurité vérifiés périodiquement, on utilise souvent des processus de Markov «multi-phases».

Il existe un grand nombre d'articles consacrés à la résolution des modèles markoviens (voir [18] et [19]).

A.3.3.3 Analyses de modèles non markoviens

Lorsque l'hypothèse d'une distribution exponentielle est assouplie, les modèles sous-jacents peuvent être résolus par diverses techniques.

- dans la théorie du renouvellement de Markov, les processus sont considérés à certains instants dans le temps où les processus sont sans mémoire. On dit qu'un processus se régénère à ces instants et qu'un autre processus est incorporé dans ces instants. Il est possible d'exprimer les équations d'état pour les processus incorporés et de déterminer les solutions du processus réel à partir de celles-ci ([3]);
- la méthode de simulation de Monte-Carlo est une méthode destinée à obtenir des estimations de la solution de problèmes mathématiques au moyen de nombres aléatoires. Cette méthode est fondée sur le calcul répété avec des variables aléatoires. L'avantage de cette approche provient du fait qu'elle permet de tenir compte du grand nombre de phénomènes qui se produisent de façon réaliste, sans complication supplémentaire dans la procédure de solution. Le principal inconvénient constaté antérieurement était l'utilisation des temps de calcul appropriés qui divergent par rapport à la précision requise. On peut déclarer désormais que cet argument est dépassé (par exemple, [12]). De plus, la simulation de Monte-Carlo fournit toujours la précision des résultats (intervalle de confiance). Tel n'est pas le cas lorsque des modèles de Markov tronqués ou agrégés sont traités.

A.3.3.4 Fonctions de récompense

Au niveau des processus stochastiques, les «taux de récompense» sont des valeurs qui sont accumulées lorsque le modèle passe du temps dans un état et les «récompenses impulsionnelles» (souvent: «assertions») sont des valeurs obtenues lorsque les transitions tirent sur certains marquages. En général, les taux de récompense peuvent être calculés en se basant sur

- des statistiques sur les états du système,
- des statistiques sur les variables du système,
- le temps passé par des jetons aux divers emplacements,
- et autres.

D'autre part, le calcul des récompenses impulsionnelles est basé sur les fréquences de tir des transitions ([3]).

Ces concepts permettent de modéliser aisément les coûts et les récompenses respectivement associés à des états de défaillance et fonctionnel. De plus, le coût des événements de réparation peut être facilement pris en compte. Ceci est utile, par exemple, lors du traitement des calculs de disponibilité de production. Un exemple d'application des fonctions de récompense dans le domaine de la sûreté de fonctionnement est développé en Annexe D.

Des représentations graphiques d'une place et d'une transition avec l'âge des récompenses sont fournies au Tableau A.2.

Tableau A.2 – Place et transition avec récompenses

Identifiant *rr* 	Identifiant *ir* 
Place avec taux de récompense	Transition (distribuée de façon exponentielle) avec récompense impulsionnelle

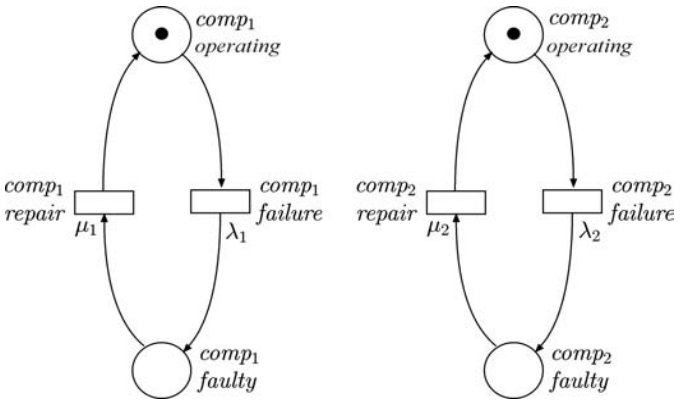
Annexe B
(informative)

Disponibilité avec redondance m sur n

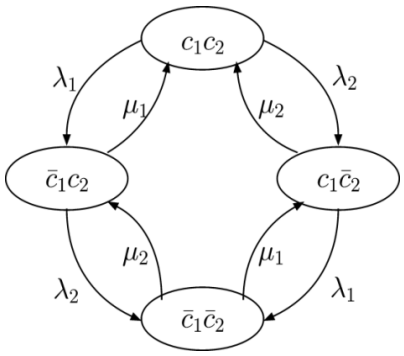
B.1 États locaux et globaux

L'aptitude d'un quelconque élément à exécuter une fonction peut être modélisée par un réseau de Petri avec un cercle de transition d'état pour exprimer sa disponibilité, par exemple les états correspondant à un élément fonctionnel ou défectueux (voir Figure A.1).

Le modèle de disponibilité du système résultant montre les ensembles combinatoires de la disponibilité locale de l'élément au moyen d'états globaux (voir Figure B.1 et Figure B.2 pour un système constitué de deux éléments et aucune liaison entre les éléments et la Figure B.3 et la Figure B.4 pour un système constitué de trois éléments sans aucune liaison). Ceux-ci seront déterminés en construisant le graphe d'atteignabilité à partir de ce réseau complet; ici, tous les états globaux du système sont représentés.



IEC 1747/12



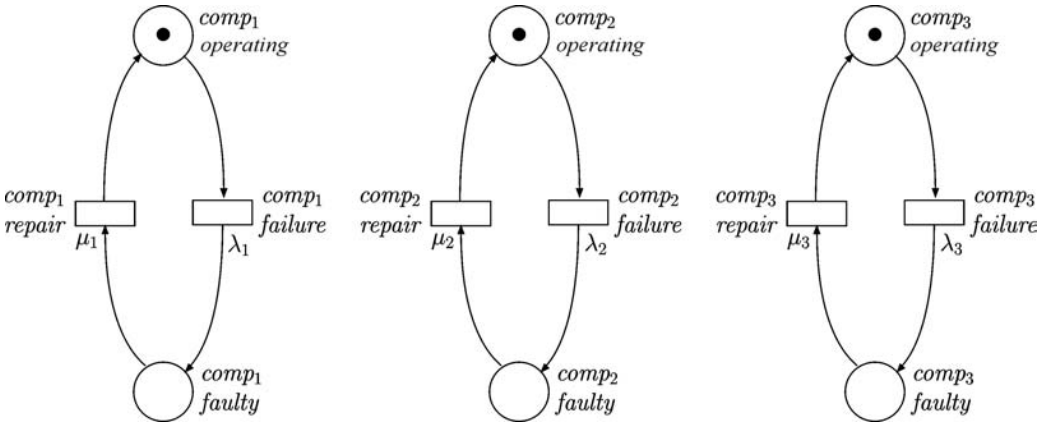
IEC 1748/12

Légende

Anglais	Français
$Comp_{1\ operating}$ / $Comp_{1\ repair}$ / $Comp_{1\ failure}$ / $Comp_{1\ faulty}$	$Comp_{1\ fonctionnel}$ / $Comp_{1\ réparation}$ / $Comp_{1\ échec}$ $Comp_{1\ défectueux}$
$Comp_{2\ operating}$ / $Comp_{2\ repair}$ / $Comp_{2\ failure}$ / $Comp_{2\ faulty}$	$Comp_{2\ fonctionnel}$ / $Comp_{2\ réparation}$ / $Comp_{2\ échec}$ $Comp_{2\ défectueux}$

Figure B.1 – Deux réseaux de disponibilité d'éléments individuels avec taux de défaillance et de réparation spécifiques

Figure B.2 – Graphe d'atteignabilité stochastique correspondant à la Figure B.1 avec états globaux ($\bar{c}_1$ est utilisé comme abréviation pour «*comp*$_1$ défectueux»)



Légende

Anglais	Français
$Comp_{1\ operating}$ / $Comp_{1\ repair}$ / $Comp_{1\ failure}$ / $Comp_{1\ faulty}$	$Comp_{1\ fonctionnel}$ / $Comp_{1\ réparation}$ / $Comp_{1\ échec}$ $Comp_{1\ défectueux}$
$Comp_{2\ operating}$ / $Comp_{2\ repair}$ / $Comp_{2\ failure}$ / $Comp_{2\ faulty}$	$Comp_{2\ fonctionnel}$ / $Comp_{2\ réparation}$ / $Comp_{2\ échec}$ $Comp_{2\ défectueux}$
$Comp_{3\ operating}$ / $Comp_{3\ repair}$ / $Comp_{3\ failure}$ / $Comp_{3\ faulty}$	$Comp_{3\ fonctionnel}$ / $Comp_{3\ réparation}$ / $Comp_{3échec}$ $Comp_{3\ défectueux}$

Figure B.3 – Trois réseaux de disponibilité d'éléments individuels avec taux de défaillance et de réparation spécifiques

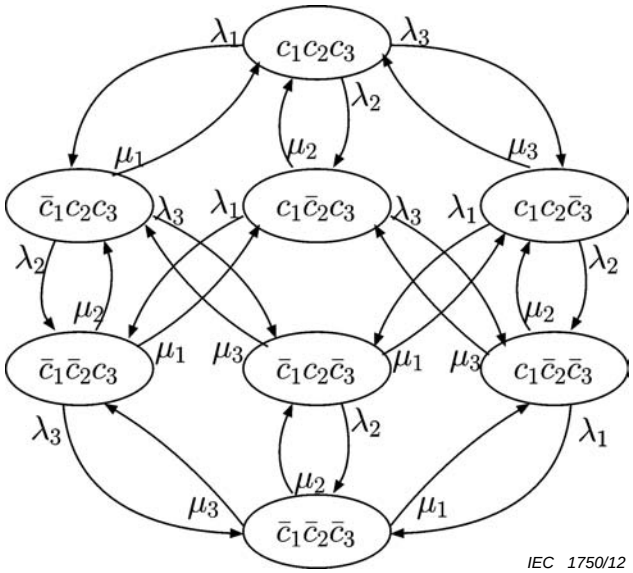


Figure B.4 – Graphe d'atteignabilité stochastique correspondant à la Figure B.3 avec états globaux ($\bar{c}_1$ est utilisé comme abréviation pour «$comp_1$ faulty»)

B.2 États globaux et structure du système

Pour la mise en œuvre d'une structure de système fonctionnel complexe qui sera exécutée par plusieurs éléments reliés (exécutant eux-mêmes des sous-fonctions), les instances correspondantes du concept de modélisation de base doivent être reliées en considérant la totalité de la structure du système, par exemple, chaîne, redondance. Selon cette structure logique, le graphe d'atteignabilité représente implicitement tous les états globaux de disponibilité et indisponibilité du système. Voir Figure B.5, Figure B.6 et Figure B.7 pour la modélisation des structures de sûreté de fonctionnement respectivement des systèmes 1 sur 3, 2 sur 3 et 3 sur 3. On peut trouver dans [20] une vue d'ensemble des techniques d'évitement de largeur et de tolérance de largeur, ainsi que d'autres techniques de construction de modèles.

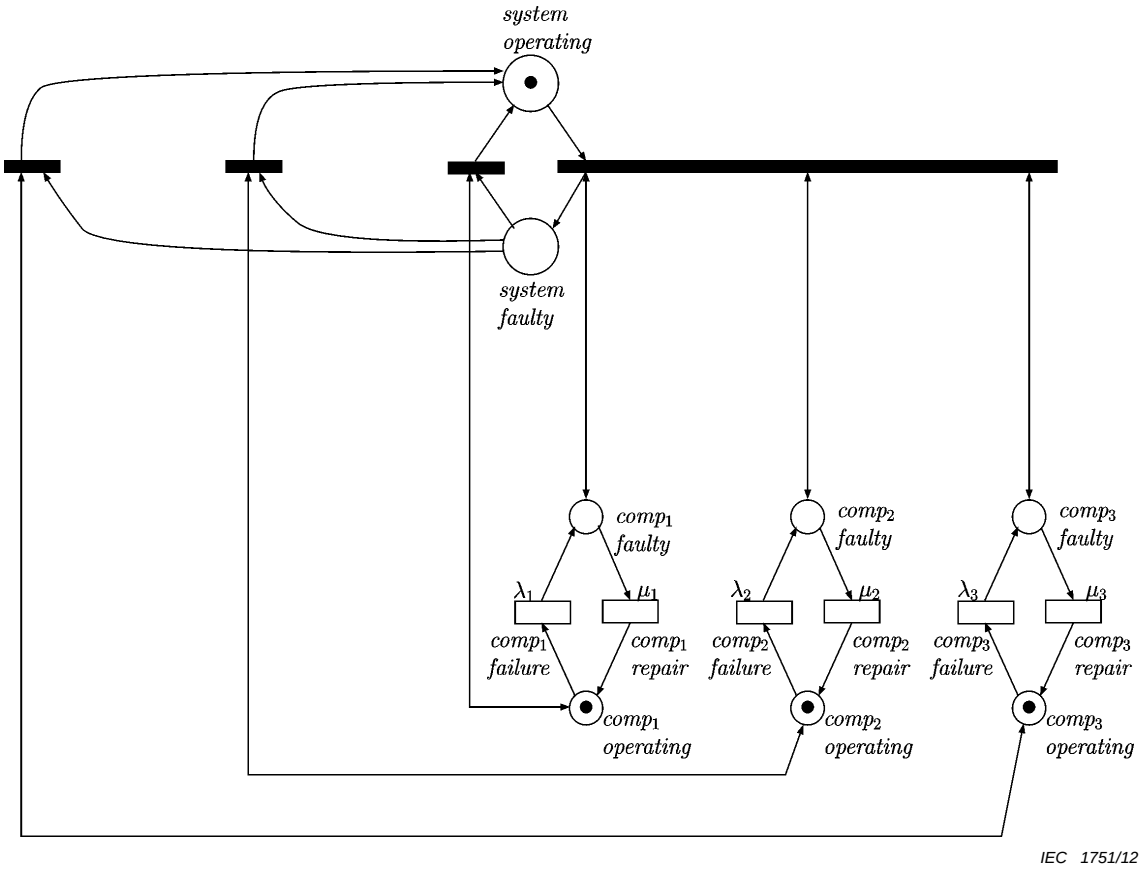


Figure B.5 – Réseau de disponibilité 1 sur 3 connecté de façon spécifique

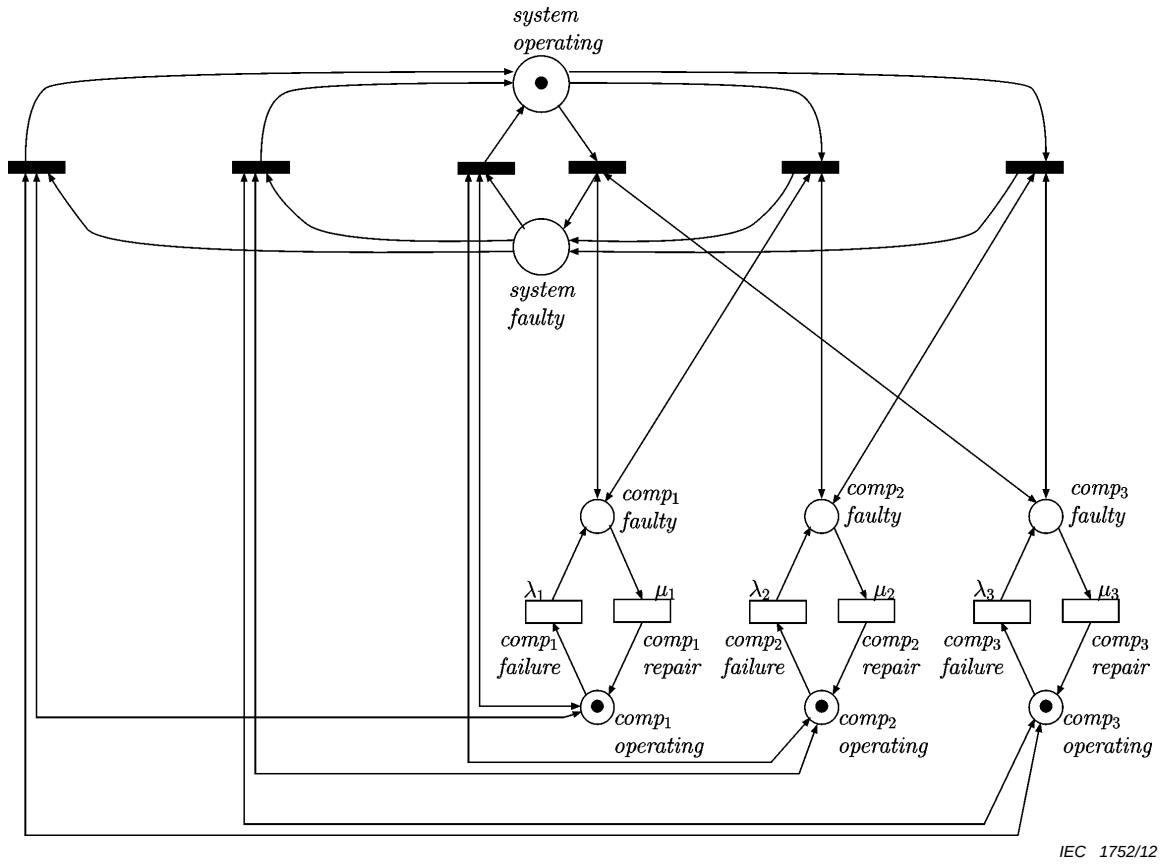


Figure B.6 – Réseau de disponibilité 2 sur 3 connecté de façon spécifique

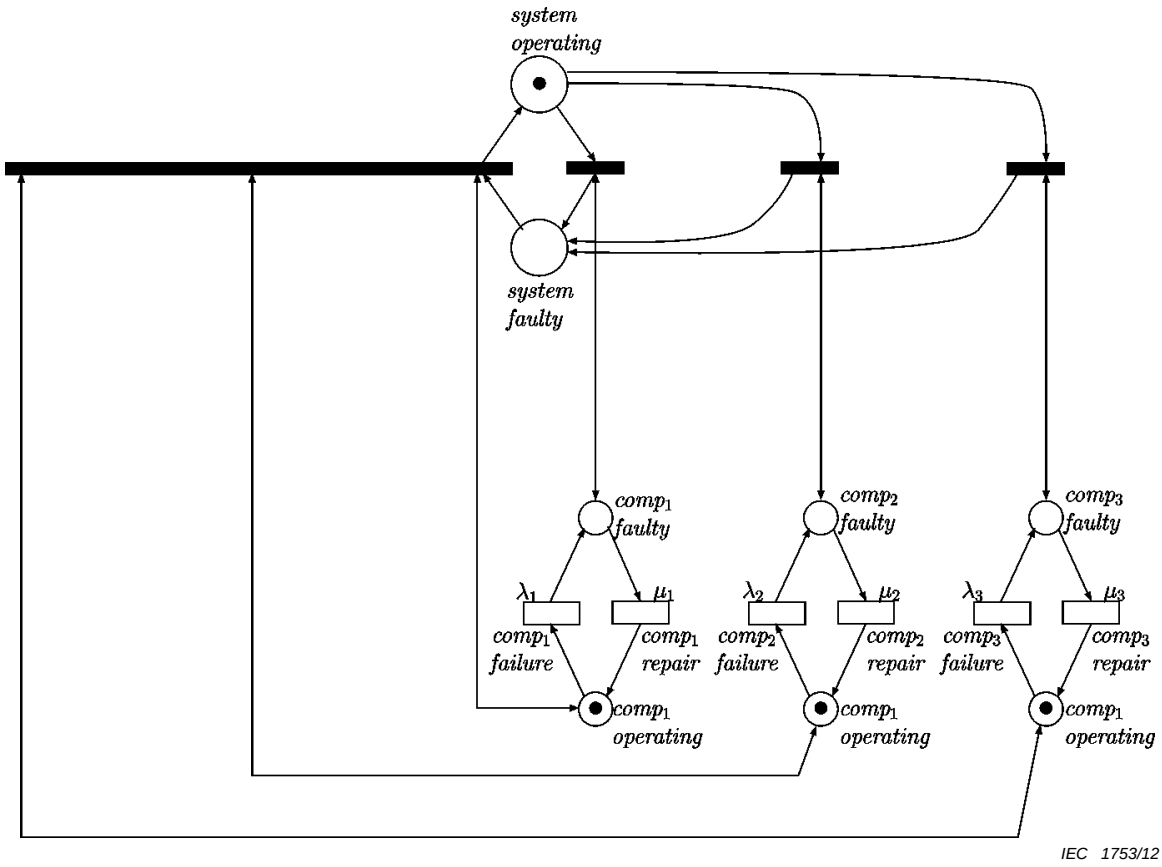


Figure B.7 – Réseau de disponibilité 3 sur 3 connecté de façon spécifique

Les états du graphe d'atteignabilité stochastique correspondant peuvent être classifiés d'une manière correspondante, voir Figure B.8. Par exemple, dans un système 3/3, le système fonctionne uniquement lorsque composant$_1$, composant$_2$ et composant$_3$ sont fonctionnels; dans un système 2/3, il existe quatre états possibles dans lesquels le système fonctionne.

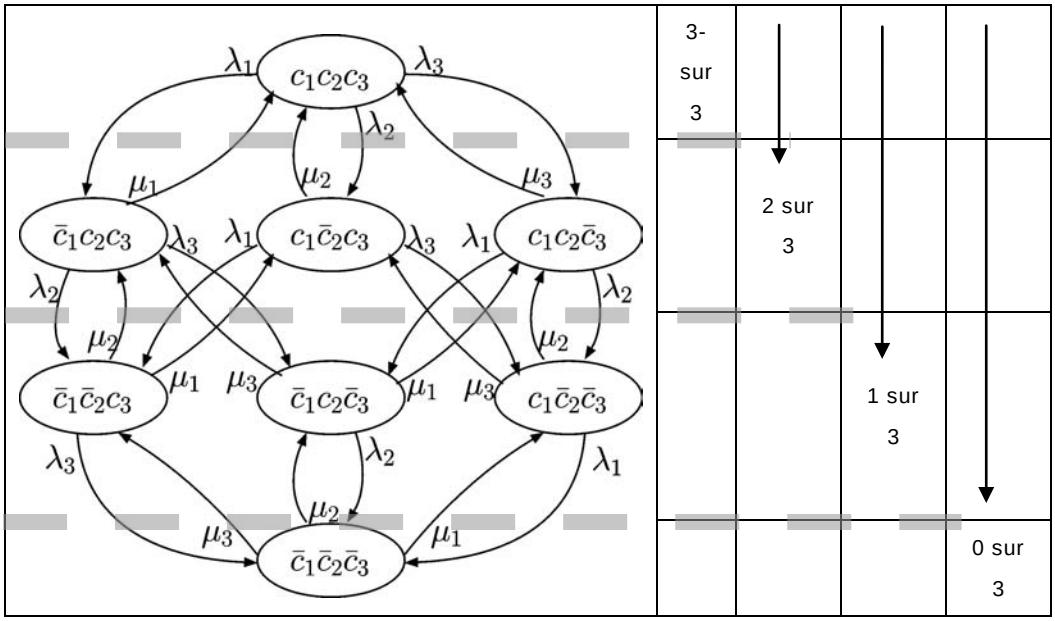


Figure B.8 – Graphe d'atteignabilité stochastique avec des états de fonctionnement spécifiques du système

En ce qui concerne la fiabilité, les systèmes correspondants peuvent être modélisés comme représenté sur les Figures B.9, B.11 et B.13. Les graphes d'atteignabilité correspondants sont respectivement présentés sur les Figures B.10, B.12 et B.14.

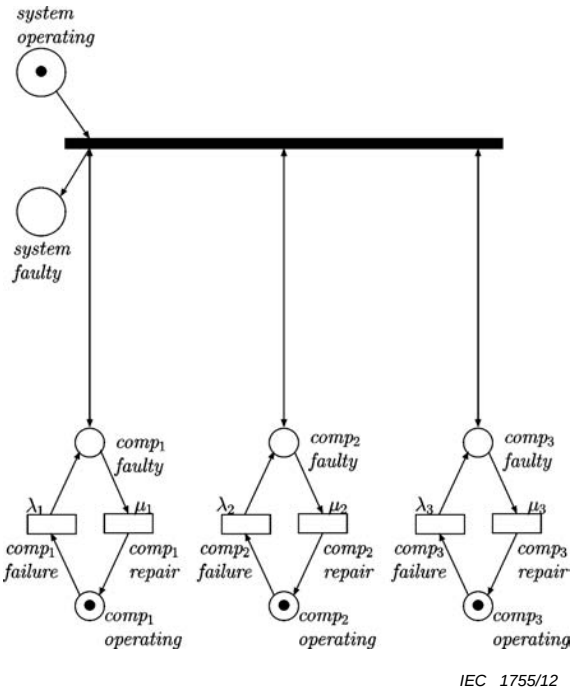


Figure B.9 – Réseau de fiabilité 1 sur 3 connecté de façon spécifique

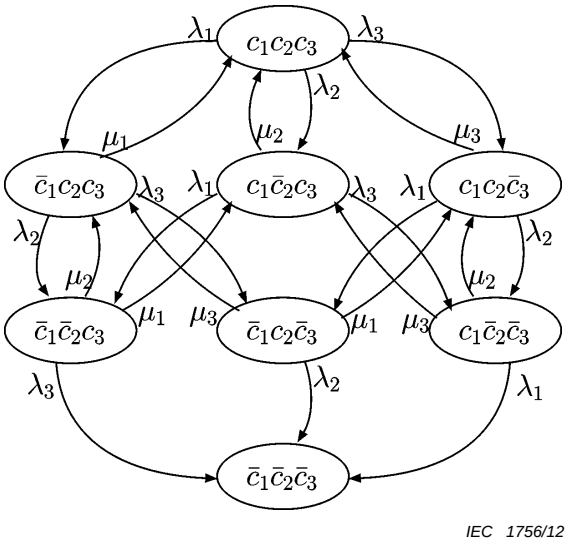


Figure B.10 – Graphe d'atteignabilité pour le réseau de la Figure B.9

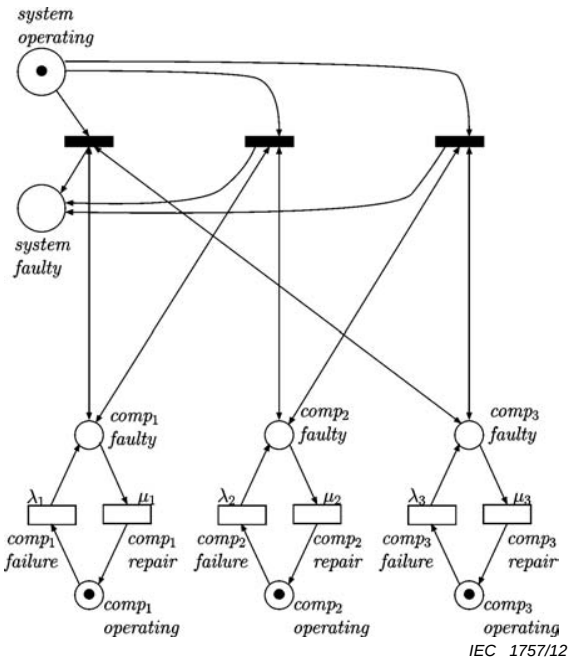


Figure B.11 – Réseau de fiabilité 2 sur 3 connecté de façon spécifique

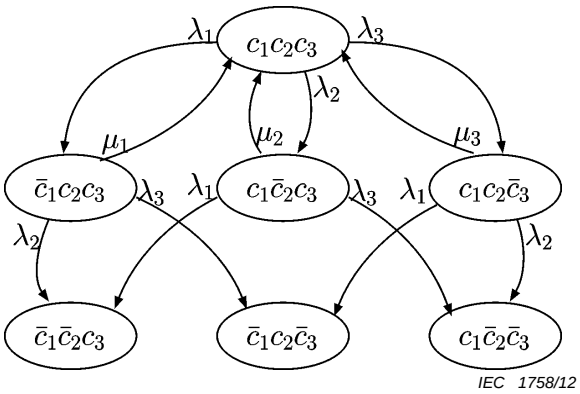


Figure B.12 – Graphe d'atteignabilité pour le réseau de la Figure B.11

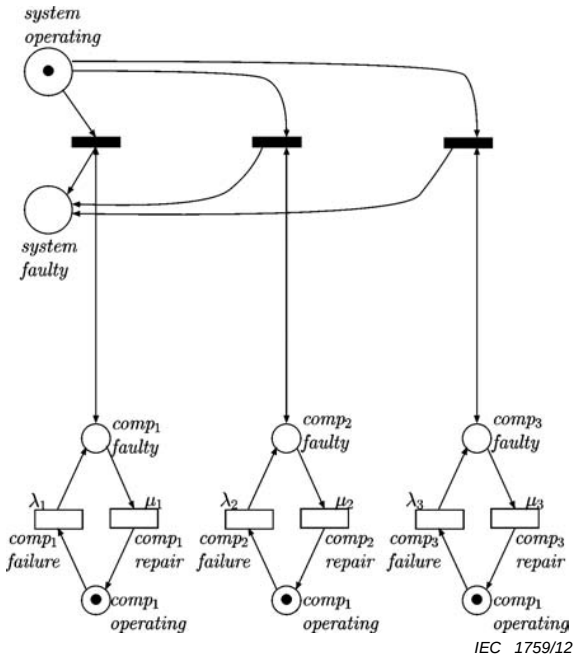


Figure B.13 – Réseau de fiabilité 3 sur 3 connecté de façon spécifique

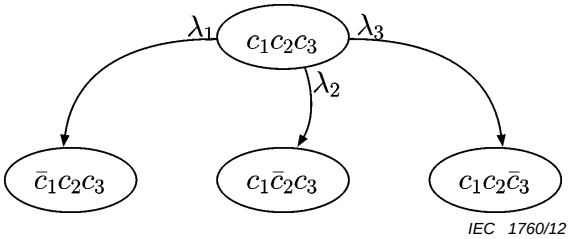


Figure B.14 – Graphe d'atteignabilité pour le réseau de la Figure B.13

Annexe C
(informative)

Exemple résumé

C.1 États locaux, globaux et globaux agrégés

En ce qui concerne la sûreté de fonctionnement, le réseau de Petri et le graphe d'atteignabilité correspondant peuvent représenter l'ensemble de ses différentes caractéristiques, à savoir, disponibilité, maintenabilité, etc.

En ce qui concerne la disponibilité et la maintenabilité, les différents états d'un élément d'un système pour exécuter une fonction peuvent être modélisés plus en détail par un réseau de Petri circulaire étendu (voir Figure C.1) qui incorpore les différents états de l'élément. Ceux-ci sont par exemple:

- fonctionnel;
- défectueux, mais non détecté comme défectueux, c'est-à-dire supposé fonctionnel;
- détecté défectueux;
- maintenu par réparation ou remplacement ou autre moyen de maintenance.

Ceci peut être réalisé en même temps que leurs quatre transitions:

- événement de défaillance;
- détection de défaillance et interruption ou arrêt;
- début de maintenance;
- transfert vers un état fonctionnel.

Noter que les trois dernières places et leurs transitions interconnectées peuvent être condensées en une super-place égale à la place «$comp_1$ faulty» de la Figure A.1. Le graphe d'atteignabilité résultant a une structure similaire simple. Il présente quatre états globaux et leurs probabilités ainsi que les transitions d'état unique avec leurs taux. En ce qui concerne la disponibilité et la sécurité, certains états globaux peuvent être condensés en un état global agrégé unique qui représente tous les états de disponibilité ou de sécurité, comme représenté à la Figure C.2.

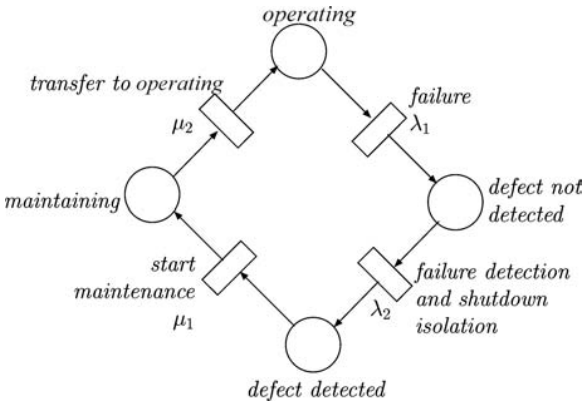


Figure C.1 – Réseau de disponibilité individuel

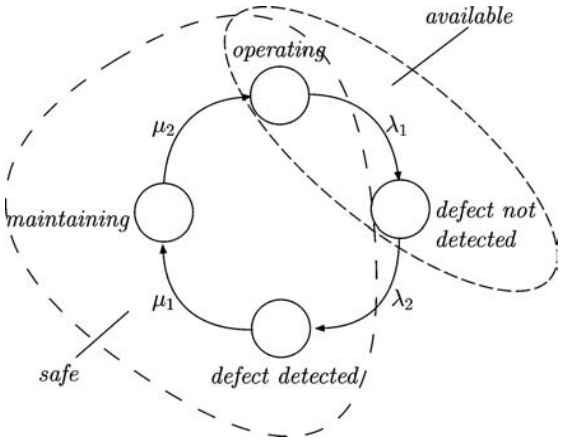


Figure C.2 – Graphe de disponibilité stochastique du réseau de la Figure C.1 avec ses états globaux et états globaux agrégés en fonction de la disponibilité et de la sécurité

Légende pour les Figures C.1 et C.2

Anglais	Français
Operating	Fonctionnel
Transfer to operating	Transfert vers fonctionnel
Maintaining	Maintenance
Start maintenance	Début maintenance
Defect detected	Défaut détecté
Failure	Défaillance
Defect not detected	Défaut non détecté
Failure detection and shutdown installation	Détection de défaillance et arrêt installation
Operating	Fonctionnel
Available	Disponible
Maintaining	Maintenance
Safe	Sûr
Defect detected	Défaut détecté
Defect not detected	Défaut non détecté

Considérant les caractéristiques de disponibilité et de sécurité, les valeurs numériques de leurs mesures peuvent nettement être représentées dans un système de coordonnées orthogonales disponibilité-sécurité. Celui-ci doit être proportionné par une mesure logarithmique de probabilité d'indisponibilité ou d'absence de sécurité, appelée respectivement potentiel de disponibilité pA et potentiel de sécurité pS, car la probabilité de disponibilité et de sécurité est généralement proche de la valeur numérique un:

$$pA = -\log(1 - A) \;\; A = \sum_{i \in A} p_i \qquad \text{(C.1)}$$

ou A est la probabilité de se trouver dans un état de l'ensemble de tous les états où le système est disponible.

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

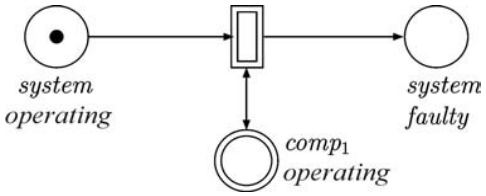
ou S est la probabilité de se trouver dans un état de l'ensemble de tous les états où le système est sûr.

Par exemple, soit A = 0,999 9, c'est-à-dire *(1-A)* = 0,000 1 et *-log(1-A)* = 4. Pour A' = 0,999 99, pA = *-log(1-A')* = 5, c'est-à-dire que pA est corrélé avec A. Il en est de même respectivement pour S et pS.

C.2 Disponibilité, fiabilité, fonction du système et hiérarchisation

En se basant sur la définition de la fiabilité, le modèle du réseau de Petri comporte la fonction requise comme conséquence de état-transition-état. Afin de réaliser la fonction requise, la disponibilité du composant lui-même sera modélisée par un cercle état-transition de fiabilité séparé pour exprimer son état fonctionnel et son état défectueux complémentaire (voir Figure A.1).

Les deux sous-réseaux sont reliés par des arcs d'essais depuis l'état fonctionnel jusqu'à l'exécution de la fonction (voir Figure C.3).



Légende: Système fonctionnel / Système défectueux / $Comp_1$ fonctionnel

Figure C.3 – Concept de modélisation de fiabilité et de fonction de base

Ce concept de modélisation de base est constitué d'une fonction logique abstraite qui est exécutée par un élément appelé «ressource» fournissant lui-même une fonctionnalité, c'est-à-dire l'aptitude à exécuter au moins la fonction requise. Le concept de modélisation de base intègre la capacité fonctionnelle et le comportement de fiabilité d'un élément (ressource).

Sur la Figure C.4, les super-transitions masquent la structure logique spécifique spécifiant la liaison n sur 3. Ici, «n» dépend du réseau caché par les super-transitions. De plus, sur la Figure C.5, les cercles état-transition de chacun des composants ont été également cachés par des super-places. Ceci signifie que les super-nœuds permettent de cacher des détails de modélisation spécifiques et permettent l'abstraction de mises en œuvre spécifiques.

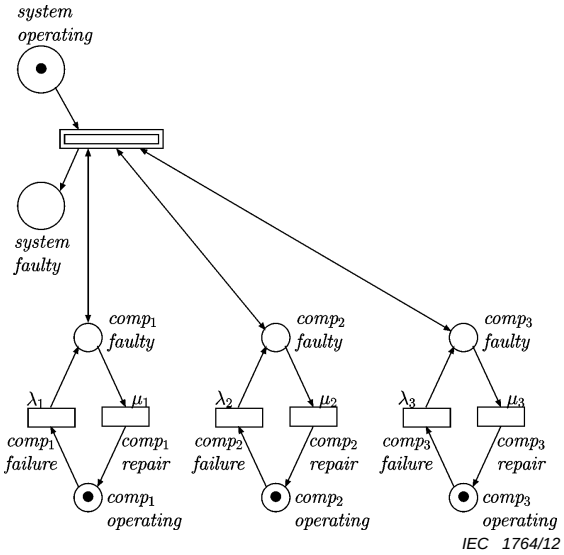


Figure C.4 – Réseau hiérarchique général avec super-transitions vers fiabilité du modèle

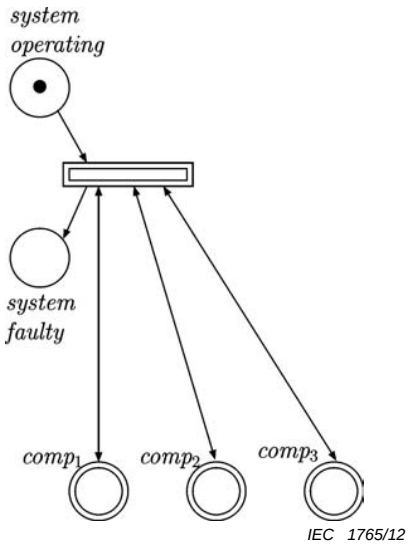


Figure C.5 – Réseau hiérarchique général avec super-transitions et super-places

Les modèles de disponibilité correspondants peuvent se trouver sur les Figures C.6 et C.7.

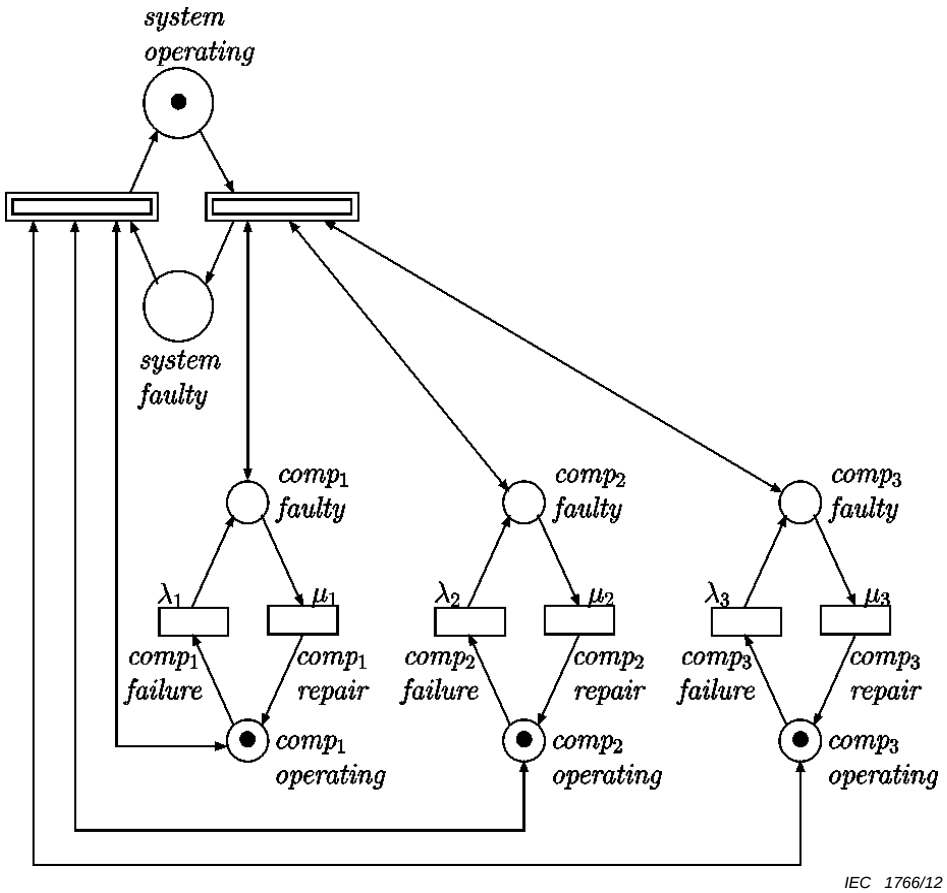


Figure C.6 – Réseau hiérarchique général avec super-transitions vers disponibilité du modèle

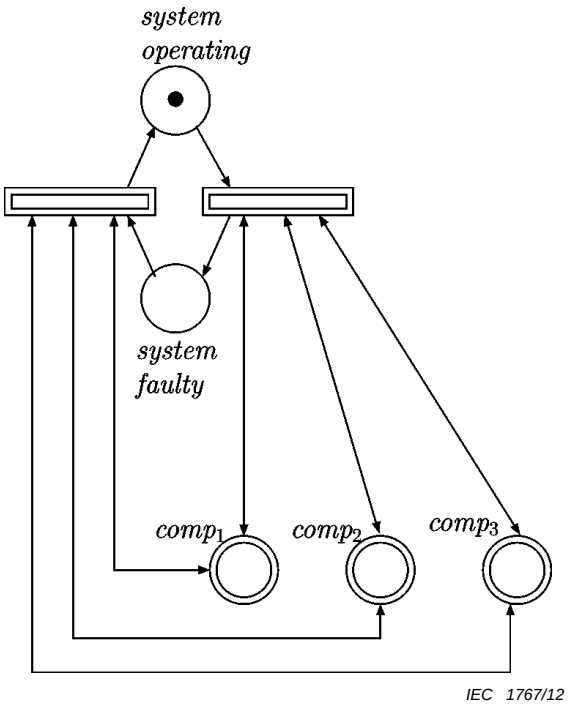


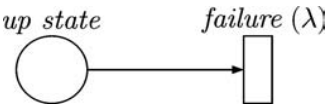
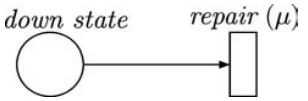
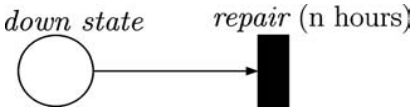
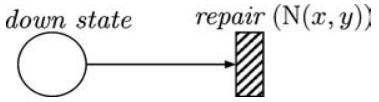
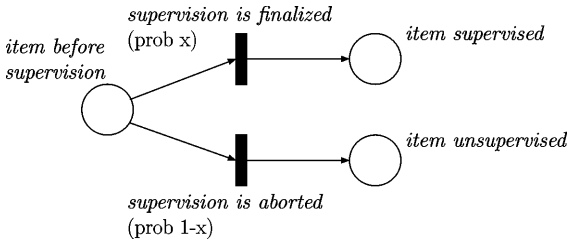
Figure C.7 – Réseau hiérarchique général avec super-transitions et super-places

Annexe D
(informative)

Modélisation de concepts types de sûreté de fonctionnement

Dans le Tableau D.1, les concepts généraux de sûreté de fonctionnement sont modélisés avec des structures de PN.

Tableau D.1 – Concepts de sûreté de fonctionnement modélisés avec des structures de PN

Concept de sûreté de fonctionnement	Solution de modélisation par PN
Défaillance avec taux de défaillance constant λ (conduisant à des temps jusqu'à défaillance distribués de façon exponentielle)	
Réparation ou rétablissement avec taux constant μ (conduisant à des temps réparation/rétablissement distribués de façon exponentielle)	
Réparation ou rétablissement (avec un temps de réparation fixe de n unités de temps)	
Réparation ou rétablissement (avec un temps de réparation à distribution normale tronquée avec une moyenne x et un écart type y)	
Maintenabilité (pour l'action de maintenance «supervision», probabilité x % de réussite de finalisation, avec $0 \leq x \leq 1$)	

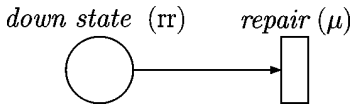
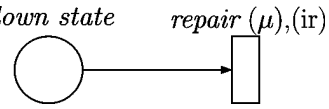
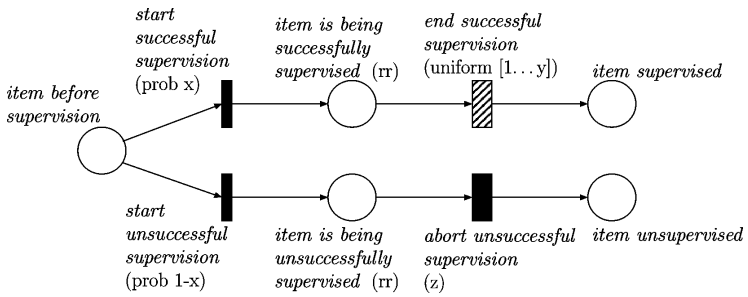
Légende

Anglais	Français
Anglais	Français
Up state	Etat actif
Failure (λ)	Ddéfaillance (λ)
Down state	Etat inactif
Repair (μ)	Réparation (μ)
Down state	Etat inactif
Repair (n hours)	Réparation (n heures)
Down state	Etat inactif
Repair ($N(x, y)$)	Réparation ($N(x, y)$)
Item before supervision	Elément avant supervision
Supervision is finalized	Supervision finalisée
Item supervised	Elément supervisé
Supervision is aborted	Supervision interrompue
Item unsupervised	Elément non supervisé

Le Tableau D.2 suggère la façon de modéliser les coûts d'états et d'événements spécifiques. Dans ce contexte, on utilise les concepts de PN de récompense: «taux de récompense» (rr)

et «récompense impulsionnelle» (ir), voir Tableau A.2. Il convient de noter qu'ici on suppose la loi normale tronquée avec un support limité [0,∞] pour la transition $N(x, y)$.

Tableau D.2 – Coûts de modélisation des états et événements

Type de coût	Solution de modélisation par PN
Coût de défaillance (les coûts sont proportionnels au temps passé cumulé dans l'état arrêté)	
Coût de réparation ou de rétablissement (les coûts sont proportionnels au nombre de réparations)	
Coût de maintenabilité (pour l'action de maintenance 'supervision', probabilité x % ($0 \le x \le 1$) de finalisation réussie et temps de supervision uniformément distribué dans l'intervalle [1…y]; les coûts de supervision accumulés apparaissent dans tous les cas)	

Légende

Anglais	Français
Down state	Etat inactif
Repair	Réparation
Item before supervision	Elément avant supervision
Start successful supervision	Début de la supervision réussie
Item is being successfully supervised	L'élément est soumis à une supervision réussie
End successful supervision (uniform)	Fin de la supervision réussie (uniforme)
Item supervised	Elément supervisé
Start unsuccessful supervision	Début de la supervision non réussie
Item is being unsuccessfully supervised	L'élément est soumis à une supervision non réussie
Abort unsuccessful supervision	Interruption de la supervision non réussie
Item unsupervised	Elément non supervisé

Annexe E
(informative)

Exemple d'un passage à niveau

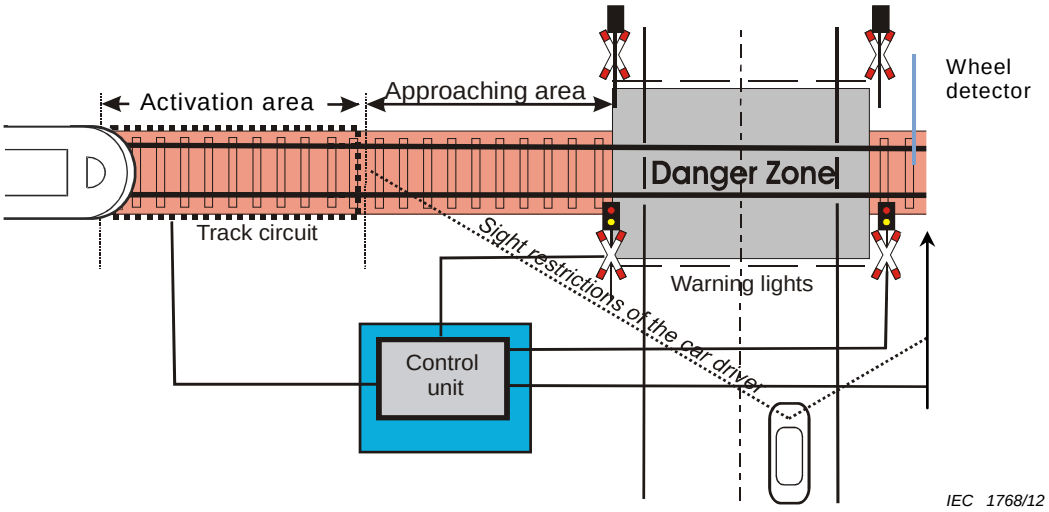
E.1 Remarques introductives

Pour présenter l'application des réseaux de Petri pour la sûreté de fonctionnement, la modélisation d'un exemple de passage à niveau (comportant des barrières) a été choisie. Dans le contexte de cet exemple, la disponibilité du passage à niveau pour le trafic routier ainsi que le risque exprimé par les taux de mortalité annuels doivent être déterminés. Par rapport à ce contexte, le taux de danger du passage à niveau, les temps d'arrivée intermédiaire des automobiles et des trains ainsi que le comportement possible des conducteurs d'automobile arrivant à un passage à niveau sont des paramètres d'intérêt probabilistes.

E.2 Description des parties et des fonctions principales du système

À la première étape, les parties et fonctions principales du système sont décrites par des moyens de description classiques, par exemple textuellement, avec des tableaux et des figures, etc. (voir 5.2.2).

a) La Figure E.1 représente l'état topologique supposé d'un passage à niveau particulier. Il contient à la fois des flux de trafic en interaction (sur rail et sur route) ainsi que l'équipement de protection contrôlant l'utilisation exclusive de la partie commune de la voie de transport. On suppose que le système représenté n'a aucune relation avec d'autres systèmes.



Légende

Anglais	Français
Activation area	Zone d'activation
Approaching area	Zone d'approche
Danger zone	Zone de danger
Control unit	Unité de contrôle
Track circuit	Circuit de voie
Warning lights	Feux d'avertissement
Wheel detector	Détecteur de roues
Sight restrictions of the car driver	Restrictions de vision du conducteur d'automobile

Figure E.1 – Exemple appliqué d'un passage à niveau et de son système de protection

b) Les parties principales du système sont l'installation, représentée par les trafics routier et ferroviaire, en interaction et le contrôle, mis en œuvre par l'équipement de protection du passage à niveau.

c) La principale fonction du trafic routier et ferroviaire est le transport en toute sécurité des personnes et des biens. On suppose des vitesses constantes des deux types de véhicules correspondant aux valeurs de vitesse maximales sur la route et sur la voie. La seule interaction possible entre les flux de trafic est constituée par la reconnaissance possible d'un véhicule ferroviaire par le conducteur du véhicule routier. Dans ce cas, le véhicule routier doit être arrêté. La reconnaissance des véhicules routiers par le conducteur du train ne conduit à aucune modification de la vitesse du train.

d) La fonction principale de l'équipement de protection est d'avertir les conducteurs de véhicules routiers de l'approche d'un train par un signal visuel. L'équipement doit donc être capable de détecter un véhicule ferroviaire en une durée définie (temps d'activation *T*AC au cours duquel le train se situe dans les zones d'activation et d'approche à la suite de quoi ce train atteint la zone de danger) qui garantit une traversée de la zone dangereuse en toute sécurité pour tous les véhicules routiers qui n'ont pas été capables de s'arrêter avant la zone dangereuse, une fois le signal d'avertissement a été activé.

E.3 Modélisation de la structure du système en se basant sur des sous-modèles de PN

À la deuxième étape, la structure du système est modélisée en se basant sur des sous-modèles de PN et sur leurs relations et en documentant ce modèle (voir 5.2.3).

La Figure E.2 représente les parties principales du modèle à considérer pour permettre l'analyse de sûreté de fonctionnement des processus de trafic dans l'exemple du passage à niveau.

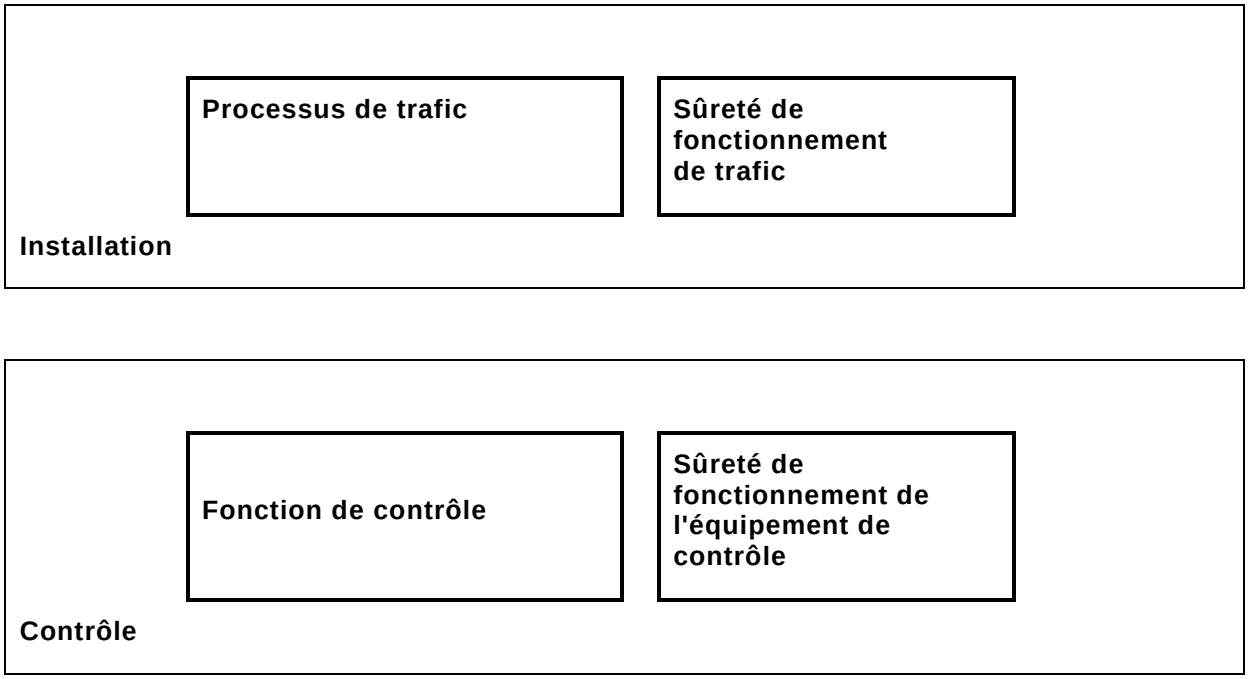
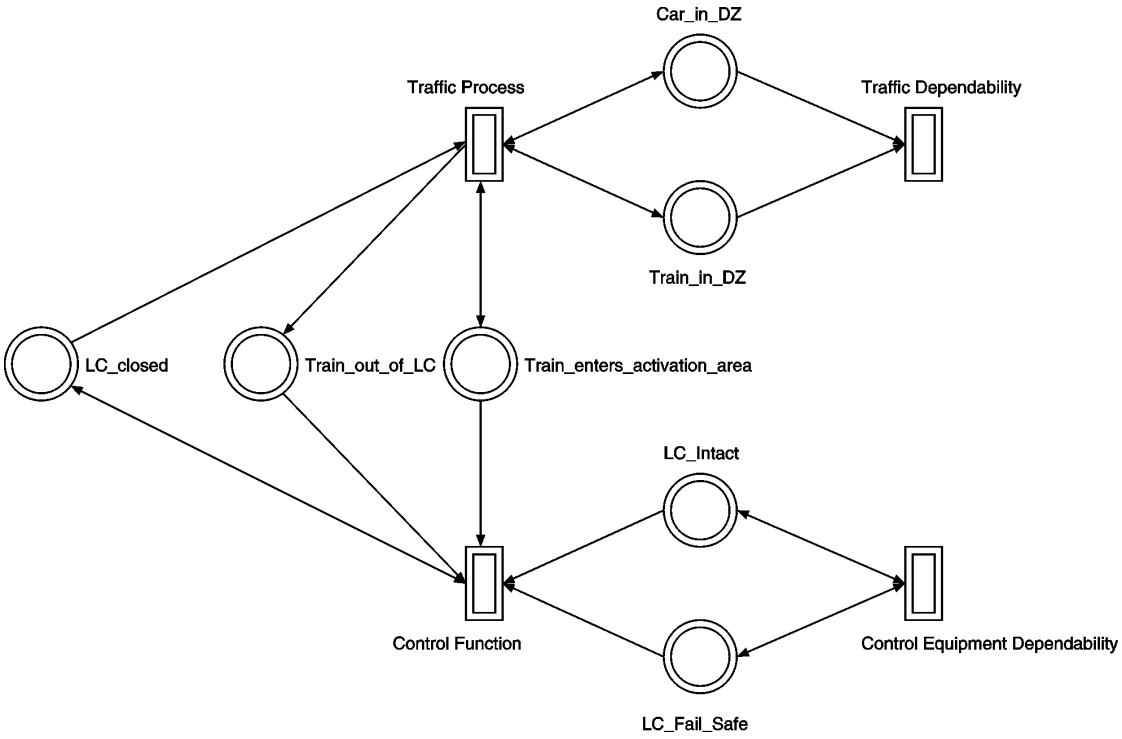


Figure E.2 – Parties principales du modèle de l'exemple du passage à niveau

La Figure E.3 représente les sous-modèles correspondants basés sur l'utilisation de super-transitions. Cette figure fait apparaître l'échange d'informations entre les parties principales du modèle.



Légende

LC passage à niveau

dz zone de danger

Anglais	Français
Car_in_DZ	Voiture_dans-DZ
Train_in_DZ	Train_en-DZ
LC_closed	LC_fermé
Train_out_of_LC	Train_en dehors du_LC
Train_enters_activation_area	Train_entre_zone_d'activité
LC_Intact	LC_Intact
LC_Fail_Safe	LC_Défaut_Sécurité
Traffic process	Processus de trafic
Traffic dependability	Sûreté de fonctionnement de trafic
Control function	Fonction de contrôle
Control equipment dependability	Sûreté de fonctionnement de l'équipement de contrôle

Figure E.3 – Sous-modèles du modèle de l'exemple du passage à niveau

Le modèle est constitué de quatre sous-modèles:

a) Un sous-modèle destiné à spécifier le processus de trafic: ce sous-modèle spécifie les automobiles et les trains s'approchant d'un passage à niveau et le quittant. Si une automobile rencontre un train dans la zone de danger, un accident se produira. Le but de ce modèle est de décrire les conséquences du comportement de différents conducteurs d'automobile sur la probabilité d'un accident. Ce modèle ne tient compte d'aucune mesure de sécurité.

b) Un sous-modèle destiné à spécifier la sûreté de fonctionnement du trafic: ici, l'occurrence possible d'accidents est explicitement modélisée. De plus, la procédure d'évacuation d'un accident est prise en compte, c'est-à-dire le temps qu'il faut pour dégager la route et la voie ferrée et les rendre à nouveau disponibles.

c) Un sous-modèle pour spécifier la fonction de contrôle: dans ce sous-réseau, le comportement de la barrière du passage à niveau est modélisé. Ici, les défaillances

conduisant à des états dangereux ne sont pas prises en compte. Il n'existe que deux états locaux: «passage à niveau ouvert» et «passage à niveau fermé». Il influe sur le comportement et, en retour, il est influencé par le processus de trafic.

d) Un sous-modèle destiné à spécifier la sûreté de fonctionnement de l'équipement de contrôle: ici, la sûreté de fonctionnement de la fonction de contrôle est modélisée. Puisque les défaillances sont prises en compte, on distingue une défaillance de sécurité et des états dangereux. Le comportement de ce sous-modèle influe sur le comportement de la fonction de contrôle.

E.4 Précision du modèle jusqu'à atteindre le niveau de détail requis

E.4.1 Généralités

À la troisième étape, le modèle de l'étape 2 est précisé jusqu'à atteindre le niveau de détail requis et, en conséquence, ce modèle précisé est documenté (voir 5.2.4). On peut diviser cette étape en précisant d'abord la structure pure du modèle et ensuite en spécifiant les paramètres individuels pour tous les nœuds du modèle.

E.4.2 Précision de la structure du modèle

Les accidents peuvent être considérés comme des conséquences de situations dangereuses survenant dans le processus de trafic. Le modèle décrit cette dépendance en se basant sur la combinaison des quatre sous-modèles suivants:

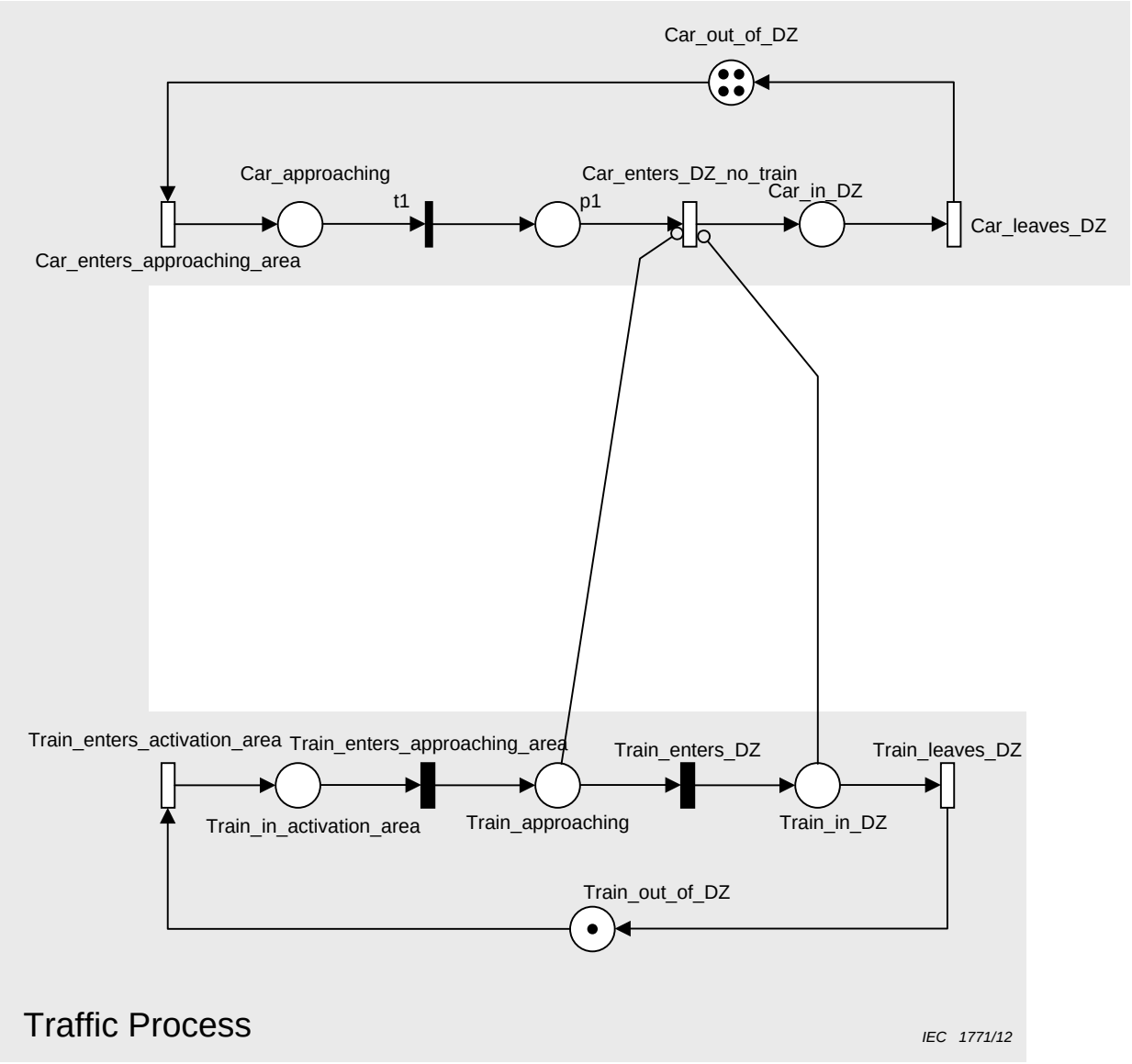
a) flux de trafic sur le passage à niveau (LC) dans le sous-modele processus de trafic;

b) survenances d'accidents dans le sous-modèle sûreté de fonctionnement du trafic;

c) opérations du LC dans le sous-modèle fonction de contrôle;

d) sources des influences dangereuses dans le sous-modèle sûreté de fonctionnement de l'équipement de contrôle.

On peut démarrer le processus de trafic en modélisant les processus de trafic «pur» automobile et ferroviaire, voir Figure E.4.

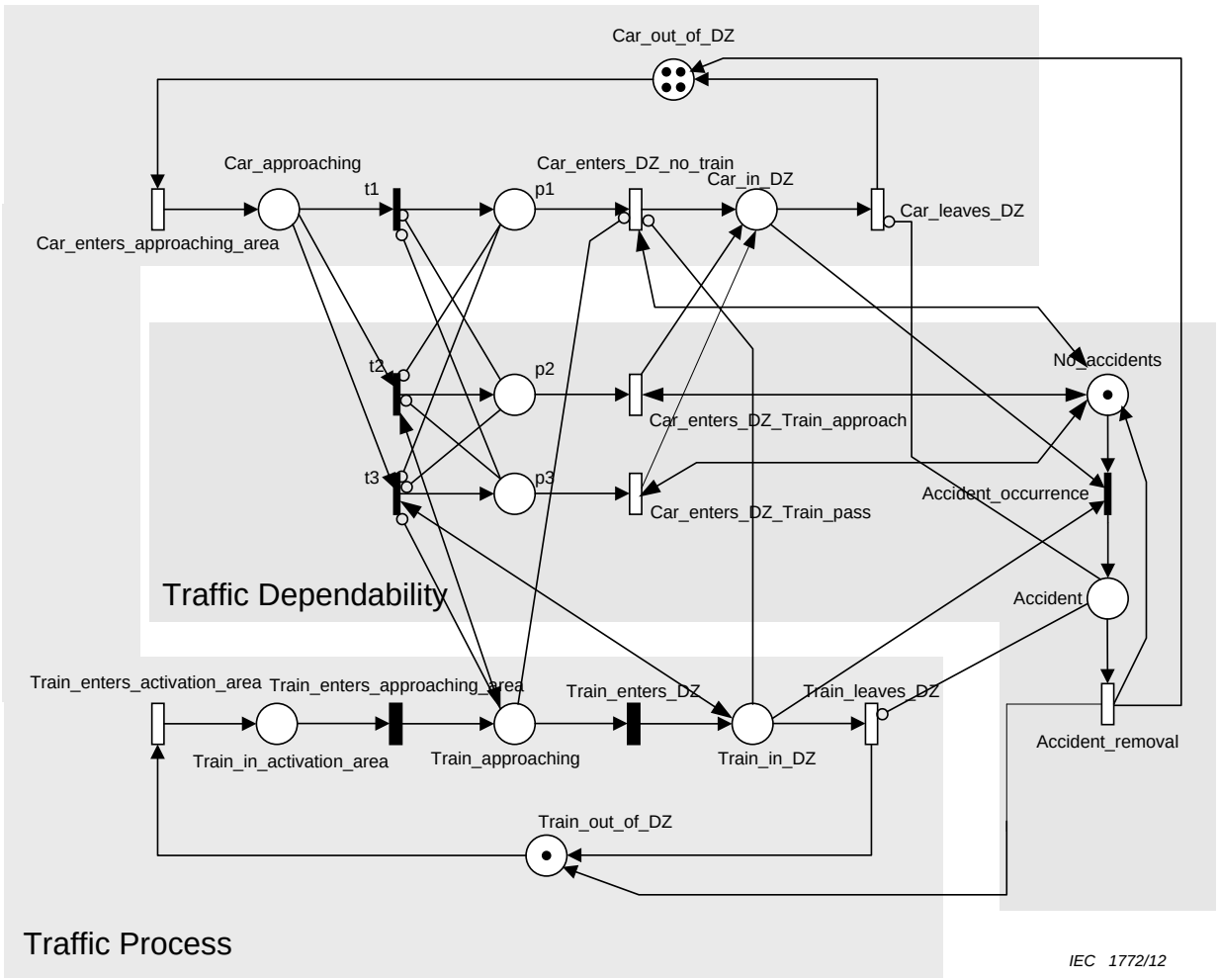


Anglais	Français
Car_out_of_DZ	Voiture_en dehors du_DZ
Car_approaching	Voiture_en approche
Car_enters_approaching_area	Voiture_entre_zone_d'approche
Car_enters_DZ_no_train	Car_entre_DZ_no_train
Car_in_DZ	Voiture_dans_DZ
Car_leaves_DZ	Voiture_depart_DZ
Train_enters_activation_area	Train_entre_zone_d'activité
Train_enters_approaching_area	Train_entre_zone_d'approche
Train_enters_DZ	Sûreté de fonctionnement de trafic
Train_leaves_DZ	Fonction de contrôle
Train_in_activation_area	Sûreté de fonctionnement de l'équipement de contrôle
Train_approaching	Train_en approche
Train_in_DZ	Train_dans_DZ
Train_out_of_DZ	Train_en dehors du_DZ

Figure E.4 – Modèle de PN des processus de trafic automobile et ferroviaire

Dans ce sous-modèle, le processus de trafic dans un «monde idéal» est modélisé: les conducteurs d'automobile ne font qu'entrer dans la zone de danger (DZ) si aucun train n'approche ou ne se trouve déjà dans la zone de danger. En conséquence, aucun accident ne va se produire. De plus, ce modèle ne tient compte d'aucune fonction de contrôle du passage à niveau.

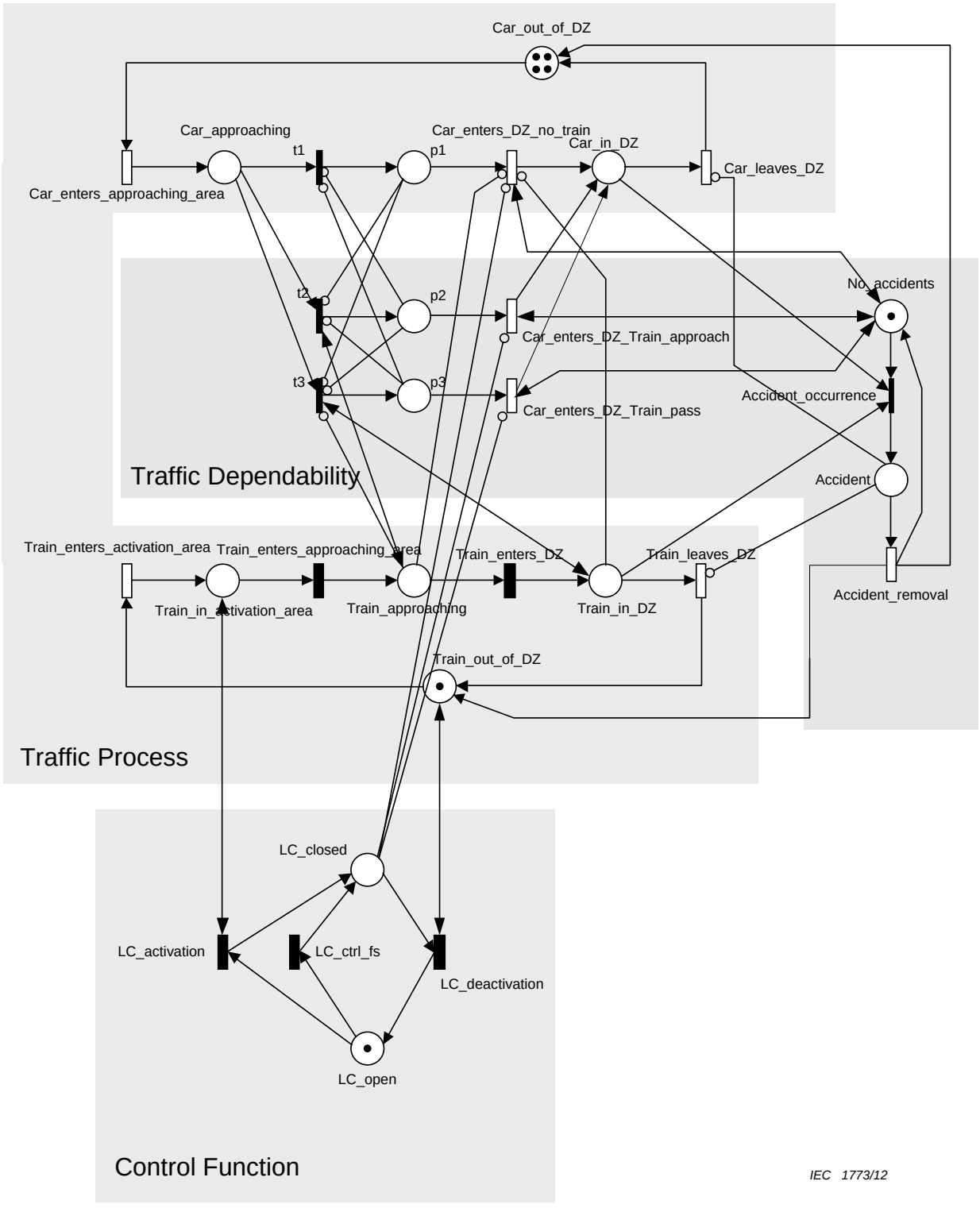
Pour tenir compte des différents types de conducteurs, le sous-modèle «sûreté de fonctionnement du trafic» est nécessaire. Dans ce sous-modèle, on considère les conducteurs qui pénètrent dans la zone de danger quand un train s'approche, ainsi que les conducteurs qui pénètrent dans la zone de danger même si un train se trouve déjà dans la zone de danger. En tenant compte de ces deux types de conducteurs, des accidents peuvent se produire. Dans ce modèle, il n'y a pourtant pas de système de contrôle, c'est-à-dire que l'on ne prend pas en considération l'existence du passage à niveau, voir Figure E.5.



Légende

Anglais	Français
Traffic dependability	Sûreté de fonctionnement du trafic
Traffic process	Processus de trafic

Figure E.5 – Modèle de PN des processus de trafic et sûreté de fonctionnement du trafic



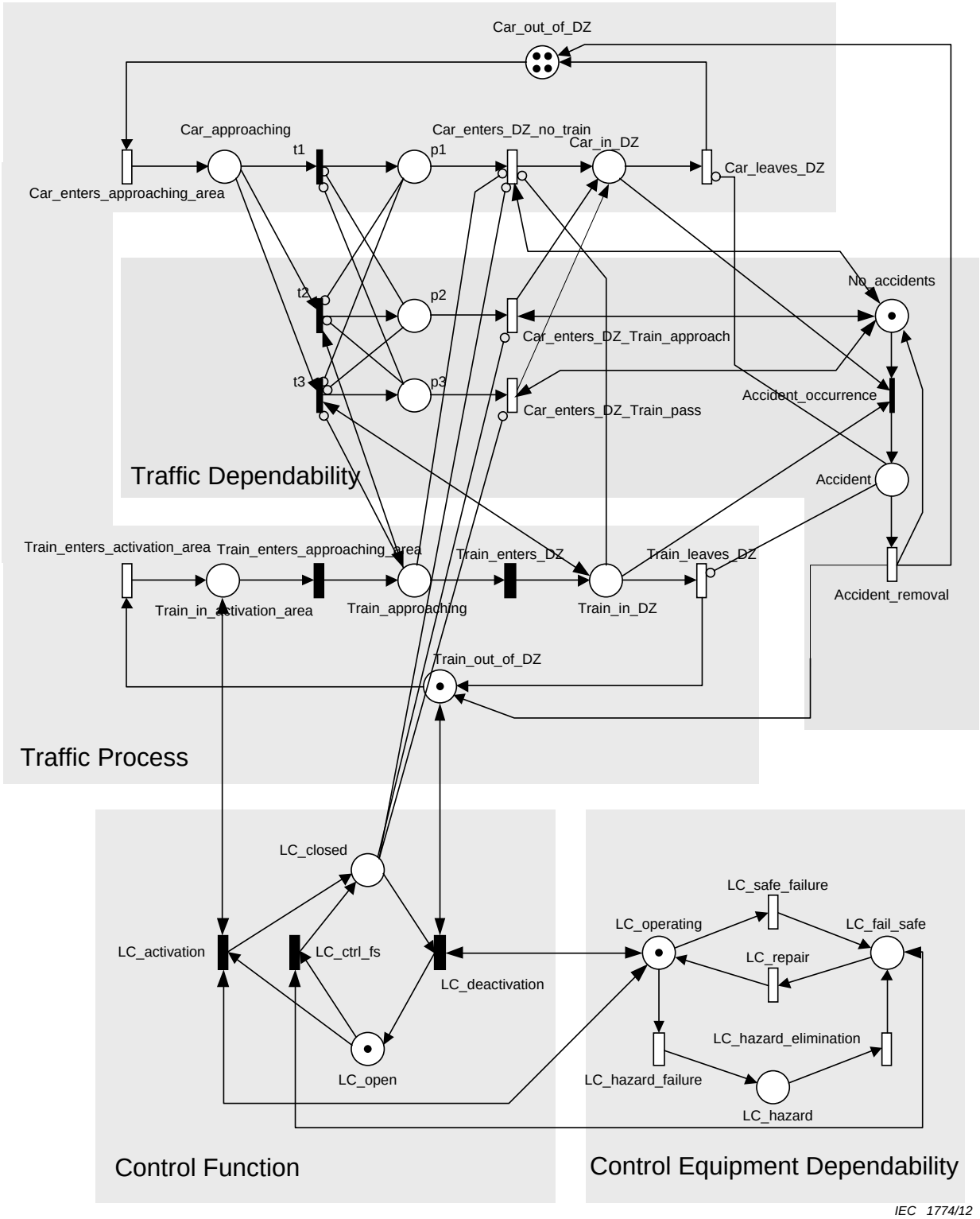
Légende

Anglais	Français
Traffic dependability	Sûreté de fonctionnement du trafic
Traffic process	Processus de trafic
Control function	Fonction de contrôle

Figure E.6 – Modèle de PN du processus de trafic avec une fonction de contrôle idéale

L'existence d'un système de contrôle de fonctionnement idéal conduit au modèle représenté à la Figure E.6. Dans ce modèle, à chaque fois qu'un train s'approche, le passage à niveau est activé et fermé. Ainsi, le modèle de la Figure E.6 ne tient pas compte des paramètres de sûreté de fonctionnement de la fonction de contrôle. On suppose que la fonction de contrôle ne présente jamais de défaillance. Dans le sous-modèle «Fonction de contrôle», par conséquent, il n'y a pas de transition probabiliste et il ne se produit donc jamais d'accident.

Enfin, la sûreté de fonctionnement de la fonction de contrôle est prise en compte. Ceci signifie qu'elle peut présenter une défaillance et en conséquence que des accidents peuvent se produire, voir Figure E.7.



Légende

Anglais	Français
Traffic dependability	Sûreté de fonctionnement du trafic
Traffic process	Processus de trafic
Control function	Fonction de contrôle
Control equipment dependability	Sûreté de fonctionnement de l'équipement de contrôle

Figure E.7 – Modèle de PN du modèle de l'exemple de passage à niveau

E.4.3 Autre explication de la structure et des paramètres du modèle

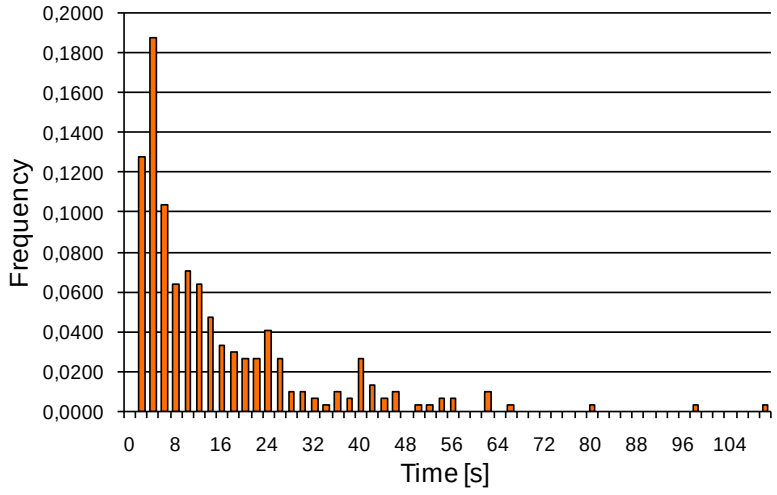
Le sous-modèle processus de trafic décrit séparément le mouvement des automobiles et des trains. Le trafic routier est représenté par six places et huit transitions (les places No_accidents et Accident ainsi que les transitions Accident_occurrence et Accident_removal n'appartiennent pas directement au Processus de trafic), dont trois sont immédiates et cinq exponentielles. Les places représentent les états pertinents du véhicule routier, comme indiqué dans le Tableau E.1.

Tableau E.1 – Places associées aux automobiles dans le sous-modèle «Processus de trafic» (voir Figure E.4)

Place	Capacité[a]	Description
Car_out_of_DZ	inf	L'automobile est à l'extérieur du système de passage à niveau. Les jetons multiples sont utilisés pour représenter un flux continu d'automobiles
Car_approaching	inf	Le conducteur de l'automobile s'approche du passage à niveau en ayant la possibilité de voir le train à l'approche
p1	1	Le conducteur de l'automobile s'approche du passage à niveau et il est prêt à pénétrer dans la zone de danger, dans la mesure où il n'y a pas de train au voisinage
Car_in_DZ	1	L'automobile est dans la zone de danger du LC
Les places Car_approaching et $p1$ ne sont séparées que par des transitions immédiates. Il n'y a ainsi aucune différence physique dans l'état de l'automobile, la différence réside dans la décision du conducteur de pénétrer ou non dans la zone de danger.		

[a] La «capacité» d'une place spécifie le nombre maximum de jetons à cette place. Une capacité de «inf(imum)» signifie qu'il n'y a aucune restriction concernant le nombre (non négatif) de jetons à cette place.

Les transitions modélisent la dynamique du mouvement de l'automobile. Le flux de trafic routier est décrit par la transition «Car_enters_approaching_area». Le paramètre de cette transition peut être évalué d'après les mesures statistiques du flux de trafic routier sur un passage à niveau particulier. La Figure E.8 représente les mesures de temps entre deux véhicules routiers sous forme d'un histogramme et la Figure E.9 représente la fonction de distribution de probabilité approchée correspondante.

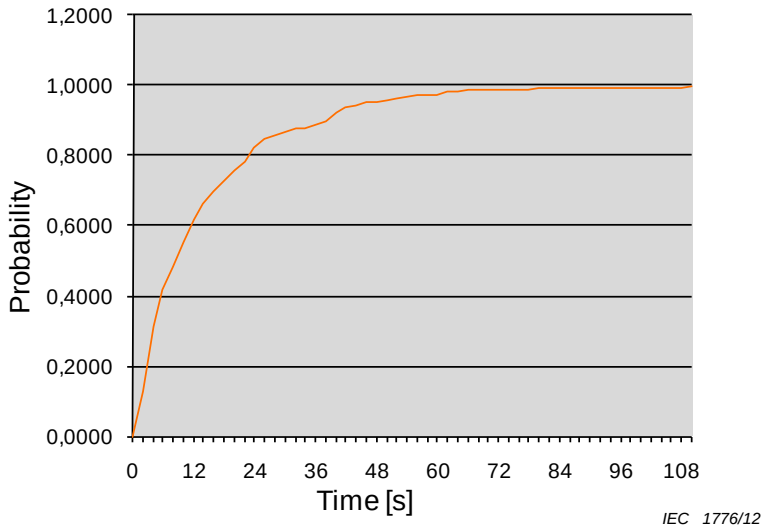


IEC 1775/12

Légende

Anglais	Français
Frequency	Fréquence
Time (s)	Temps (s)

Figure E.8 – Mesures recueillies du flux de trafic routier d'un passage à niveau particulier: Intervalle de temps entre deux automobiles parvenant au passage à niveau



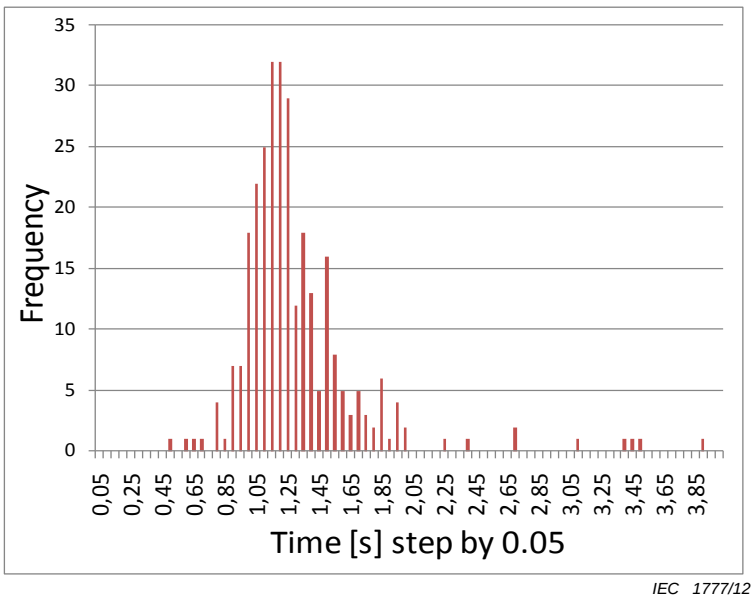
Légende

Anglais	Français
Probability	Probabilité
Time (s)	Temps (s)

Figure E.9 – Fonction de distribution de probabilité approchée basée sur les mesures indiquées à la Figure E.5

Les mesures présentées ont été approchées par une distribution exponentielle avec une valeur de l'espérance de 16,2 s (0,27 min).

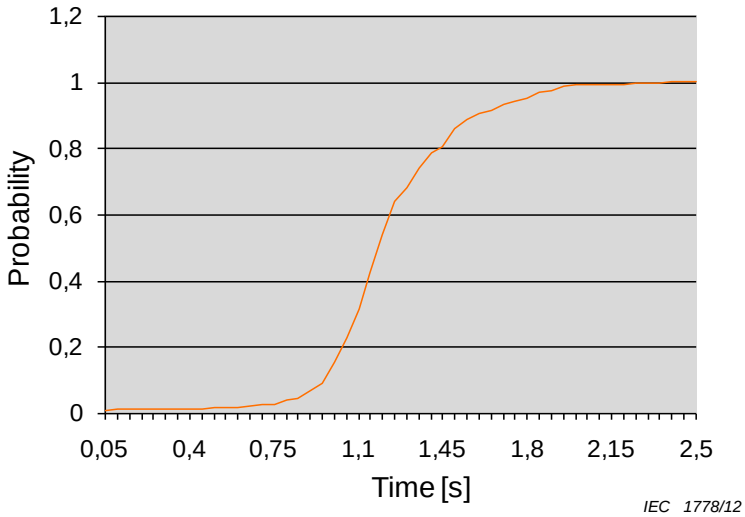
On a évalué de façon similaire le paramètre de la transition «Car_leaves_DZ». La Figure E.10 représente les mesures sur site du passage à niveau particulier.



Légende

Anglais	Français
Frequency	Fréquence
Time (s) step by 0,05	Temps (s) pas de 0,05

Figure E.10 – Mesures recueillies du temps passé par un véhicule routier dans la zone de danger du passage à niveau



Légende

Anglais	Français
Probability	Probabilité
Time (s)	Temps (s)

Figure E.11 – Fonction de distribution de probabilité approchée basée sur les mesures indiquées à la Figure E.10

Comme on peut le voir, la distribution correspondante n'est pas exponentielle. Puisque ce paramètre a une influence significative sur la probabilité de l'occurrence d'un accident, il est recommandé de considérer le temps du véhicule routier le plus lent comme moyenne de la fonction de distribution exponentielle au lieu de ne tenir compte que de l'occupation moyenne dans le temps de la zone de danger. En conséquence, le paramètre de la transition «Car_leaves_DZ» a été fixé à 3,96 s (0,066 min).

Le modèle présenté envisage les différents comportements possibles des conducteurs de véhicules routiers lorsqu'ils s'approchent d'un passage à niveau dans le cas où aucun avertissement n'est donné par l'équipement de protection (par exemple, en raison d'une défaillance). Selon des estimations d'experts, dans ce cas 50 % des conducteurs pénètrent dans la zone de danger du passage à niveau même s'ils observent un train à l'approche: le tir de la transition $t2$ conduit à l'activation de «Car_enters_DZ_Train»_approach (en supposant que le LC n'est pas fermé). Avec une probabilité de 45%, $t1$ tire et marque la place $p1$. La transition «Car_enters_DZ_no_train» n'est activée que s'il n'y a pas de train dans la zone d'approche ou dans la zone de danger. 5 % des conducteurs entrent quand même dans la zone de danger si un train franchit le passage à niveau (par exemple, en raison d'une mauvaise visibilité ou des conditions de freinage). Ces considérations sont modélisées par une pondération des transitions immédiates $t1$, $t2$ et $t3$ en conséquence. Les poids sont appliqués lorsque deux transitions immédiates ou plus sont activées simultanément. Tel est le cas par exemple pour $t1$ et $t2$ lorsqu'une automobile et un train se trouvent dans la zone d'approche (les places «Car_approaching» et «Train_approaching» sont marquées

Les paramètres de toutes les transitions décrivant la dynamique du trafic routier (avec d'autres explications) sont résumés dans le Tableau E.2.

Tableau E.2 – Transitions associées au trafic routier dans le sous-modèle «Processus de trafic» et Sûreté de fonctionnement du trafic (voir Figure E.7)

Nom de la transition	Concept de temps	Paramètre de poids	Temps min	Description
Car_enters_approaching_area	Distribué de façon exponentielle	–	0,27	Décrit le flux de trafic routier (voir ci-dessus)
*t*1	Immédiat	95	–	Décrit le cas d'un véhicule routier pénétrant dans la zone de danger uniquement s'il n'y a aucun train
*t*2	Immédiat	95	–	Décrit le cas d'un véhicule routier pénétrant dans la zone de danger si un train est à l'approche et qu'aucun avertissement n'est fourni
*t*3	Immédiat	5	–	Décrit le cas d'un véhicule routier pénétrant dans la zone de danger si un train passe et qu'aucun avertissement n'est fourni
Car_enters_DZ_no_train	Distribué de façon exponentielle		0,1	Décrit le temps passé par une automobile dans la zone d'approche
Car_enters_DZ_Train_approach	Distribué de façon exponentielle		0,1	Décrit le temps passé par une automobile dans la zone d'approche
Car_enters_DZ_Train_pass	Distribué de façon exponentielle		0,1	Décrit le temps passé par une automobile dans la zone d'approche
Car_leaves_DZ	Distribué de façon exponentielle		0,066	Décrit le temps passé par une automobile dans la zone de danger

Les paramètres de tous les places décrivant la dynamique du trafic routier (y compris d'autres explications) sont résumés dans le Tableau E.3.

Tableau E.3 – Places associés au trafic ferroviaire dans le sous-modèle «Processus de trafic» (voir Figure E.7)

Nom de la place	Capacité	Description
Train_out_of_DZ	1	Le train est à l'extérieur du système de passage à niveau.
Train_in_activation_area	1	Le train est dans la zone dans laquelle l'équipement de protection du passage à niveau (feux d'avertissement) est activé et l'avertissement visuel démarre
Train_approaching	1	Le train est dans la zone dans laquelle il est visible par un conducteur d'automobile dans la zone d'approche
Train_in_DZ	1	Le train est dans la zone de danger du LC

La dynamique du trafic ferroviaire est décrite par les transitions. Le flux du trafic ferroviaire est décrit par la transition «Train_enters_activation_area», dont le paramètre est évalué en se basant sur l'analyse des horaires. Dans l'exemple donné, la fréquence moyenne des trains est de deux trains par heure, en supposant une distribution exponentielle des temps entre deux trains. L'exemple suppose en outre la même vitesse de tous les trains conduisant à des temps constants passés par la tête du train dans la zone d'activation et d'approche du passage à niveau (T_{AC} = const. 0,133 min + 0,166 min). Le temps passé dans la zone de

danger dépend de la longueur du train. Sa variation est évaluée en fonction de la distribution exponentielle avec le temps moyen de 0,3 min.

Les distributions de la transition du trafic ferroviaire et les significations des paramètres sont résumées dans le Tableau E.4.

Tableau E.4 – Transitions associées au trafic ferroviaire dans le sous-modèle «Processus de trafic» (voir Figure E.7)

Nom de la transition	Concept de temps	Temps min	Description
Train_enters_activation_area	Distribué de façon exponentielle	30	Décrit le flux de trafic ferroviaire
Train_enters_approaching_area	Déterministe	0,133	Décrit le temps passé par le train dans la zone d'activation (active l'avertissement)
Train_enters_DZ	Déterministe	0,166	Décrit le temps passé par le train dans la zone d'approche (visible par le conducteur de l'automobile)
Train_leaves_DZ	Distribué de façon exponentielle	0,5	Décrit le temps passé par le train dans la zone de danger

L'interaction entre les processus de trafic routier et ferroviaire est représentée par les arcs d'essai et inhibiteur. Ceux-ci sont particulièrement utilisés lors de la modélisation de la décision du conducteur de l'automobile d'entrer dans la zone de danger et de l'interaction entre les automobiles (les transitions immédiates $t1$, $t2$ et $t3$ ne peuvent être activées que lorsqu'aucune automobile n'est prête à pénétrer dans la zone de danger aux places $p1$, $p2$ et $p3$).

La possibilité d'un accident est modélisée dans le sous-modèle «Sûreté de fonctionnement *du trafic»*. L'occurrence est modélisée par deux arcs provenant des places «Car_in_DZ» et «Train_in_DZ» du sous-réseau «Processus de trafic». Aucune temporalité n'est supposée, tous les accidents sont considérés comme des conséquences logiques immédiates de la présence simultanée des véhicules routier et ferroviaire dans la zone de danger du passage à niveau. La procédure d'évacuation d'accident est supposée avoir une durée distribuée de façon exponentielle de 2 h (120 min) en moyenne. Pendant l'évacuation de l'accident, le passage à niveau n'est pas disponible pour le trafic ferroviaire et routier (modélisé par des inhibiteurs correspondants). La signification des places et transitions ainsi que de leurs paramètres est résumée dans le Tableau E.5 et le Tableau E.6.

Tableau E.5 – Places dans le sous-modèle «Sûreté de fonctionnement du trafic» (voir Figure E.7)

Nom de la place	Capacité	Description
No_Accidents	1	Aucun accident dans la zone de danger
Accident	1	Accident dans la zone de danger
$p2$	1	Le conducteur de l'automobile s'approche du passage à niveau et il est prêt à entrer dans la zone de danger, même si un train s'approche (tant que le dispositif d'avertissement n'est pas actif)
$p3$	1	Le conducteur de l'automobile s'approche du passage à niveau et il est prêt à entrer dans la zone de danger, même si un train la traverse (tant que le dispositif d'avertissement n'est pas actif)

Tableau E.6 – Transitions dans le sous-modèle «Sûreté de fonctionnement du trafic» (voir Figure E.7)

Nom de la transition	Concept de temps	Poids	Temps min	Description
Accident_occurrence	Immédiat	1		Décrit les conséquences logiques de l'occupation simultanée de la zone de danger par une automobile et un train
Accident_removal	Distribué de façon exponentielle	–	120	Décrit la durée de la procédure d'évacuation de l'accident

Le sous-réseau «Fonction de contrôle» décrit l'influence de l'équipement de protection du passage à niveau sur les processus de trafic. Les places «LC_open» et «LC_closed» représentent les états principaux de l'équipement du système. L'activation de l'équipement (transition «LC_activation») est modélisée par l'arc d'essai relié avec la place du modèle de processus de trafic, représentant le train dans la zone d'activation. Une autre cause d'activation est la détection d'une défaillance de l'équipement modélisée par un état de défaillance sûr dans le sous-réseau «Sûreté de fonctionnement de l'équipement de contrôle» (par exemple, une défaillance du détecteur de roues pour désactiver l'équipement de protection ou un type quelconque d'autre défaillance détectée). La désactivation de l'équipement («LC_deactivation») survient au moment où le train a quitté la zone de danger (liaison de l'arc d'essai avec la place «Train_out_of_DZ»), tant que l'équipement est dans l'état fonctionnel. Le modèle suppose que, si l'équipement de protection du passage à niveau est dans l'état d'avertissement, aucun conducteur d'automobile ne décide de pénétrer dans la zone de danger (modélisée par des inhibiteurs vers les transitions dans le sous-réseau processus de trafic). D'autres extensions du modèle peuvent également être utilisées pour modéliser un comportement plus réaliste des conducteurs d'automobile, en considérant également la violation des feux d'avertissement. Le Tableau E.7 et le Tableau E.8 résument la signification et les paramètres des places et des transitions appartenant au sous-modèle «Fonction de contrôle».

Tableau E.7 – Places dans le sous-modèle «Fonction de contrôle» (voir Figure E.7)

Nom de la place	Capacité	Description
LC_open	1	Le LC est dans l'état passif, l'avertissement pour l'usager de la route est désactivé
LC_closed	1	Le LC est dans l'état actif, l'avertissement pour l'usager de la route est activé

Tableau E.8 – Transitions dans le sous-modèle «Fonction de contrôle» (voir Figure E.7)

Nom de la transition	Concept de temps	Paramètre de poids	Description
LC_activation	Immédiat	1	Décrit l'activation de l'équipement de protection du LC
LC_deactivation	Immédiat	1	Décrit la désactivation de l'équipement de protection du LC
LC_ctrl_fs	Immédiat	1	Décrit l'activation du LC due à la détection d'une défaillance de l'équipement de protection

Les états de sûreté de fonctionnement internes de l'équipement de protection du passage à niveau sont modélisés dans le sous-réseau «Sûreté de fonctionnement de l'équipement de contrôle». Il est constitué des trois états pertinents représentant l'état fonctionnel, de sécurité positive et de danger. Les transitions exponentielles modélisent les changements d'état possibles (de façon similaire à l'utilisation d'une chaîne de Markov). L'utilisation des arcs d'essai de la Figure E.3 pour relier les sous-réseaux de l'équipement de la fonction de

contrôle modélise l'influence des états de sûreté de fonctionnement sur la fonctionnalité de l'équipement de protection du passage à niveau. On peut voir en particulier que, si l'équipement de protection est dans un état de danger (par exemple, une défaillance du dispositif de détection de train ou un quelconque type de défaillance non détectée de l'équipement de protection), aucune activation de l'avertissement des conducteurs de véhicules routiers n'est possible.

Le Tableau E.9 et le Tableau E.10 résument la signification et les paramètres des places et des transitions appartenant au sous-modèle «Sûreté de fonctionnement de l'équipement de contrôle».

Tableau E.9 – Places dans le sous-modèle «Sûreté de fonctionnement de l'équipement de contrôle» (voir Figure E.7)

Nom de la place	Capacité	Description
LC_operating	1	Le LC est dans l'état fonctionnel, la fonctionnalité de l'équipement de protection du LC (activation et désactivation) est entièrement disponible
LC_fail_safe	1	Le LC est dans l'état de défaillance sûr, l'équipement de protection du LC est dans un état sûr, l'avertissement pour l'usager de la route est activé
LC_hazard	1	Le LC est dans un état de danger, la fonctionnalité de l'équipement de protection du LC (activation et désactivation) n'est pas disponible

Tableau E.10 – Transitions dans le sous-modèle «Sûreté de fonctionnement de l'‘équipement de contrôle» (voir Figure E.7)

Nom de la transition	Concept de temps	Temps min	Description
LC_hazard_failure	Distribué de façon exponentielle	6×10^6	Décrit le temps écoulé avant occurrence de la défaillance dangereuse de l'équipement de protection du LC
LC_safe_failure	Distribué de façon exponentielle	6×10^5	Décrit le temps écoulé avant occurrence de la défaillance de sécurité de l'équipement de protection du LC
LC_hazard_elimination	Distribué de façon exponentielle	360	Décrit le temps écoulé avant détection d'une défaillance dangereuse de l'équipement de protection du LC
LC_repair	Distribué de façon exponentielle	240	Décrit le temps nécessaire pour la réparation de l'équipement de protection du LC (après une défaillance détectée)

Le paramètre temporel de la transition «LC_hazard_failure» est le temps moyen jusqu'à une défaillance dangereuse et correspond au niveau d'intégrité de sécurité de l'équipement de protection du passage à niveau. Le modèle suppose que le taux d'occurrence de la défaillance du système de sécurité est dix fois plus grand que l'occurrence du taux de danger. Le paramètre de la transition «LC_hazard_elimination» peut être obtenu par analyse de données statistiques ou en tenant compte du retard le plus long entre deux trains (en supposant, par exemple, la détection d'une défaillance dangereuse de l'équipement de protection du passage à niveau *LC* par le conducteur du train) qui était de 6 h (360 min). Le paramètre temporel de la transition «LC_repair» est estimé à 4 h (240 min), ce qui représente le temps de réparation après détection d'une défaillance, incluant l'activation, le trajet et le temps de réparation de l'équipe de maintenance.

Il n'existe pas de protection de transition spécifique définie; ceci signifie que toutes les protections peuvent être considérées comme «vraies» ou «satisfaites». La politique de préemption est «répétition de préemption différente» pour toutes les transitions.

E.5 Analyse du modèle pour obtenir les résultats d'intérêt

Dans la quatrième étape, le modèle est analysé pour obtenir les résultats d'intérêt et les analyses sont documentées (voir 5.2.5).

La tâche d'analyse quantitative consiste à étudier l'espace d'état du modèle. Le graphe d'atteignabilité qualitatif du réseau a été généré. Le graphe correspondant possède 300 états. On n'a pas visualisé ce graphe, on a construit en remplacement un graphe agrégé.

La tâche de l'analyse quantitative consiste à évaluer le taux d'occurrence des accidents en fonction des paramètres des transitions utilisées dans le modèle (par exemple, le nombre de trains ou de véhicules routiers par heure, la durée du temps d'activation utilisé T_{AC}, le niveau d'intégrité de sécurité (SIL, voir la EN 50126 [21]) de l'équipement de protection, etc.). Puisqu'elles sont distribuées de façon exponentielle comme les transitions synchronisées et les transitions causales déterminées, les simulations de Monte-Carlo conduisent aux résultats d'analyse.

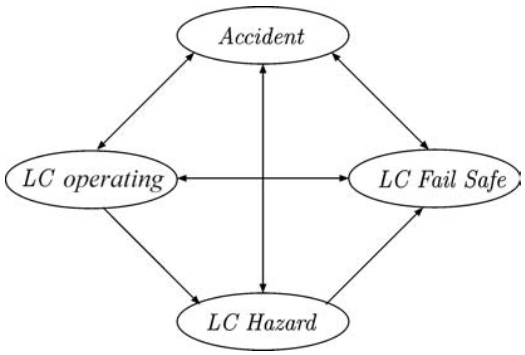
Toutes les analyses ont été effectuées avec PN-Tool TimeNet dans la version 4.0 (voir [22]) et ont été confirmées en utilisant l'outil *π-Tool* [23].

Le calcul a été effectué sur un CPU (Unité centrale de traitement) Pentium 4 Intel à 2,4 GHz sur une carte «Asus P4B533» avec 1 024 Mo de mémoire vive. Puisque le modèle tient compte de la «suppression des accidents», un seul historique a dû être simulé. La durée de l'historique était d'environ 250 millions d'années et le temps de calcul d'environ 120 jours. Celui-ci a pu être raccourci à quelques jours par un prétraitement mathématique n'ayant aucune influence sur le résultat de la simulation.

E.6 Représentation et interprétation des résultats

À la cinquième étape, les résultats des analyses sont représentés et interprétés et cette représentation est documentée (voir 5.2.6).

En ce qui concerne l'analyse quantitative, en utilisant la visualisation par le graphe d'atteignabilité agrégé, on peut vérifier certaines relations évidentes entre les états globaux principaux. À titre d'exemple, le RG agrégé de la Figure E.12 révèle l'occurrence d'états de sûreté de fonctionnement de l'équipement de protection du passage à niveau et leur relation avec l'état d'accident. Comme on peut le voir, le graphe confirme la séquence modélisée des états de sûreté de fonctionnement (fonctionnel, danger, sécurité positive) et montre qu'un accident peut se produire indépendamment de l'état de sûreté de fonctionnement de l'équipement de protection du passage à niveau (dans tous les cas, la situation telle qu'une automobile a pénétré dans la zone de danger et y est resté jusqu'à ce qu'un train soit arrivé peut se produire) comme représenté à la Figure E.12.



IEC 1779/12

Légende

Anglais	Français
Accident	Accident
LC operating	LC fonctionnel
LC fail safe	LC sécurité positive
LC hazard	LC danger

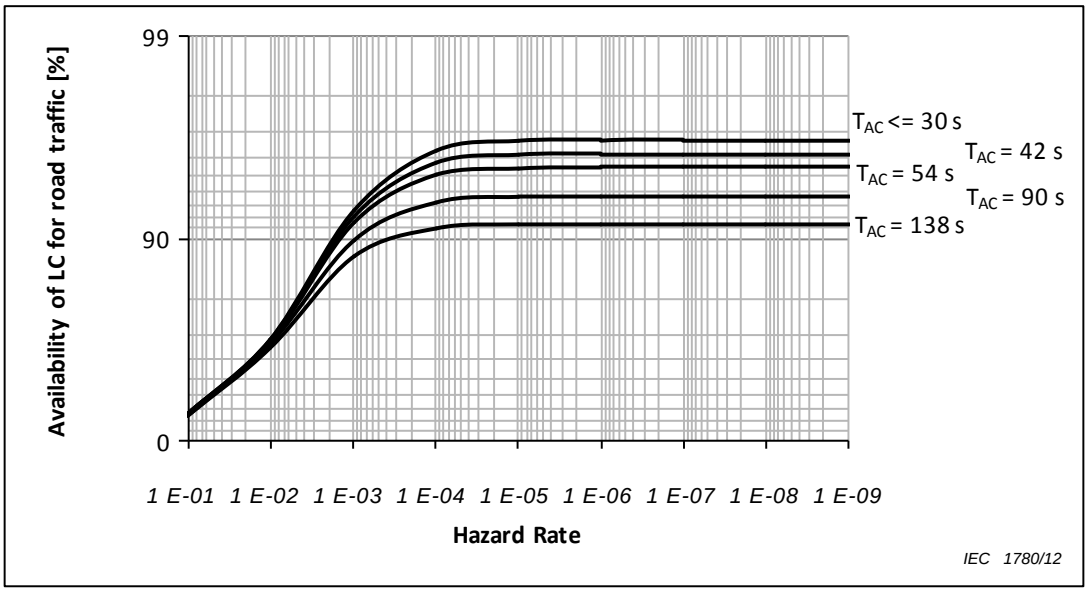
Figure E.12 – RG agrégé et informations relatives aux états correspondants

Dans le Tableau E.11, le nombre d'états du modèle de PN résumé dans l'état agrégé correspondant (dû à l'état booléen) est indiqué.

Tableau E.11 – Spécification des conditions booléennes pour les états à résumer dans un état agrégé

Nom de l'état agrégé	Condition booléenne	Nombre d'états du RG (ordinaires) qui sont résumés dans l'état du RG agrégé
Accident	m(accident) >= 1	39
LC_operating	m(LC_operating) >= 1 ∧m(accident) = 0	71
LC Hazard	m(LC_hazard) >= 1 ∧m(accident) = 0	100
LC Fail Safe	m(LC_fail_safe) >= 1 ∧m(accident) = 0	90
NOTE '∧ ' spécifie le «et» logique; m(place) représente le marquage d'une place, c'est-à-dire le nombre de jetons à cette place		

Les résultats de l'analyse quantitative peuvent être utilisés d'une part pour évaluer la disponibilité du passage à niveau pour le trafic routier. On s'attend à ce que la disponibilité augmente en diminuant le temps d'activation T_{AC} de l'avertissement du passage à niveau (avant l'arrivée du train) ainsi qu'en diminuant le taux d'occurrence de défaillance dangereuse (en particulier en raison de l'hypothèse telle que dans ce cas également le taux d'occurrence de la défaillance de sécurité positive augmente linéairement (1:10)). La Figure E.13 confirme ces attentes.

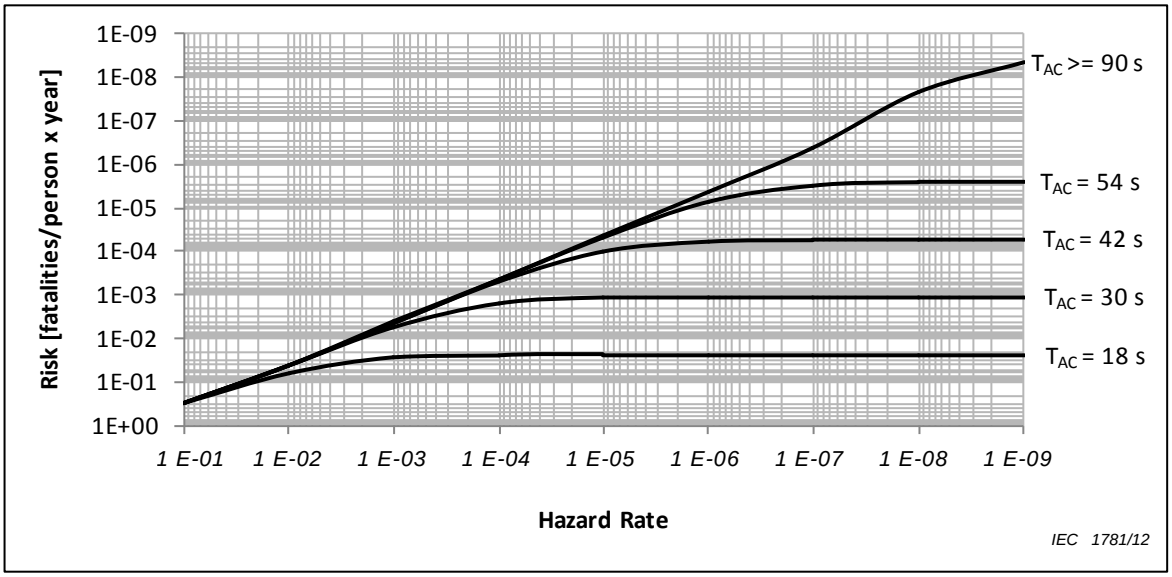


Légende

Anglais	Français
Availability of LC for road traffic (%)	Disponibilité du LC pour le trafic routier (%)
Hazard rate	Taux de danger

Figure E.13 – Résultats de l'analyse quantitative montrant la disponibilité moyenne du passage à niveau pour les usagers du trafic routier en fonction du taux de danger de l'équipement de protection pour différents temps d'activation et d'approche utilisés T_{AC}

D'autre part, les résultats de l'analyse quantitative peuvent être utilisés pour évaluer la sécurité du trafic routier. Considérant le flux de données des véhicules routiers et l'occupation moyenne d'une automobile par 1,5 personne et le taux de mortalité de 1, le taux d'occurrence des accidents obtenu peut être utilisé pour évaluer le risque individuel des usagers de la route au passage à niveau (mortalité des usagers de la route sous forme de taux de mortalité par personne et par an). La Figure E.14 montre la dépendance du risque des utilisateurs individuels de la route par rapport au temps d'activation utilisé T_{AC} et le taux de danger de l'équipement de protection du passage à niveau.

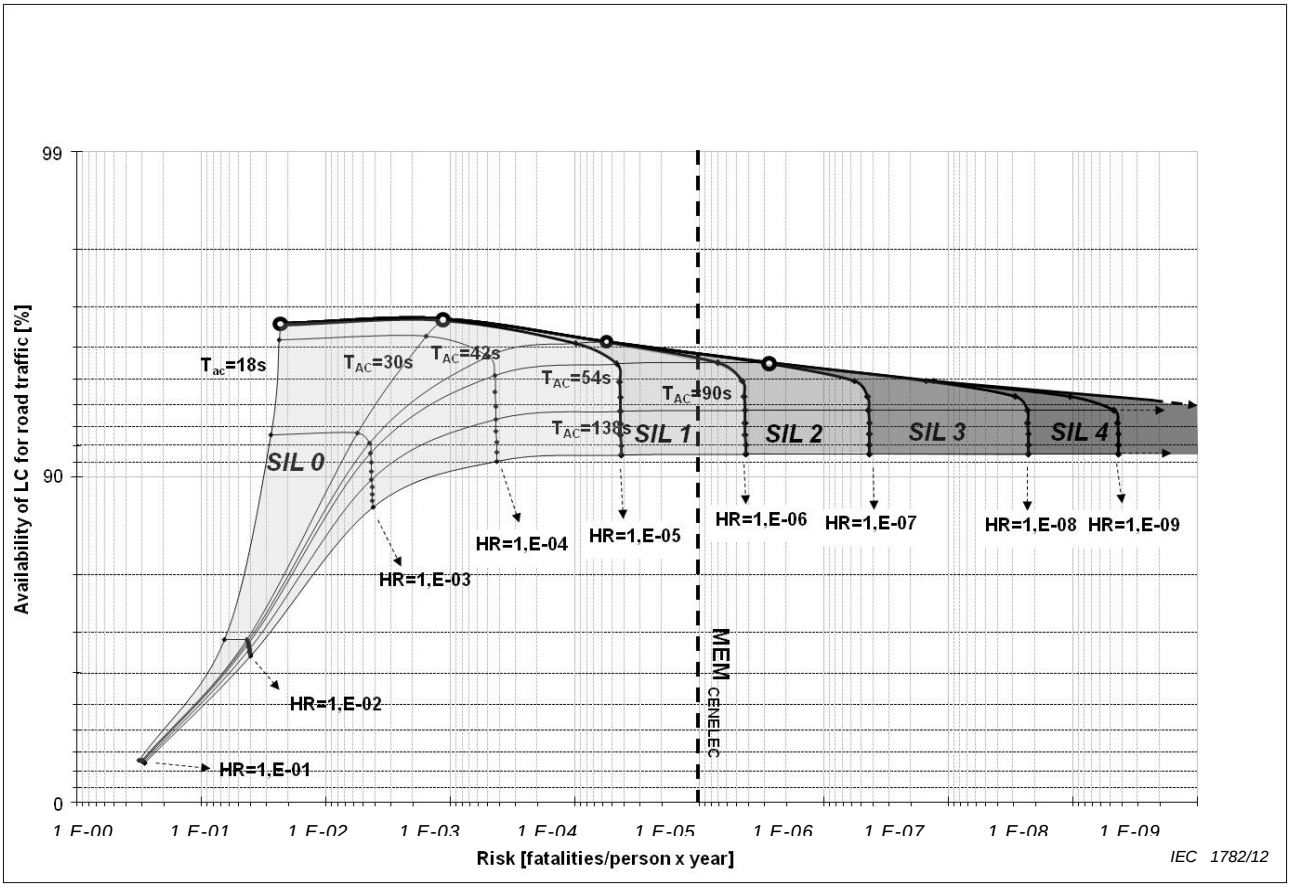


Légende

Anglais	Français
Risk (fatalities/person x year)	Risque (mortalité/personne par an)
Hazard rate	Taux de danger

Figure E.14 – Résultats de l'analyse quantitative montrant le risque individuel des usagers du passage à niveau en fonction du taux de danger de l'équipement de protection pour différents temps d'activation et d'approche utilisés T_{AC}

Comme on peut le voir sur la Figure E.13 et la Figure E.14, certaines améliorations techniques conduisant à l'augmentation du niveau d'intégrité de sécurité (diminution du taux de danger) sont inutiles et ne peuvent conduire qu'à augmenter les coûts de développement et de production du système. La visualisation des résultats de l'analyse quantitative par le diagramme sécurité/disponibilité représenté à la Figure E.15 montre une possibilité appropriée de prospects d'optimisation.



Légende

Anglais	Français
Availability of LC for road traffic (%)	Disponibilité du LC pour le trafic routier (%)
Risk (fatalities/person x year)	Risque (mortalité/personne par an)

Figure E.15 – Diagramme de sécurité de disponibilité basé sur les résultats quantitatifs de l'analyse du modèle représenté à la Figure E.13 et à la Figure E.14

La Figure E.15 montre que la valeur optimale du temps d'activation T_{AC} est d'environ 54 s, ce qui permet de diminuer le risque pour que le véhicule routier ne soit pas capable de se dégager de manière satisfaisante de la zone de danger. Cette valeur montre la possibilité d'utiliser la technique du niveau d'intégrité de sécurité 1 (HR = 1 E-5 – 1 E-6), fournissant un taux de disponibilité du passage à niveau pour le trafic routier de 94,5 %, et le risque individuel de 1 E-5 décès par personne et par an (la valeur d'acceptation du risque $MEM_{CENELEC}$ est la «Mortalité endogène minimale» donnée par EN 50126 [21]).

Bibliographie

Références citées par l'ordre d'apparition

[1] PETRI, C.A., *Kommunikation mit Automaten*. Schriften des Instituts für instrumentelle Mathematik, Bonn, 1962

[2] CEI 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

[3] GERMAN, R., *Performance Analysis of Communication Systems – Modeling 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] CEI 60050-151:2001, *Vocabulaire Electrotechnique International – Partie 151:Dispositifs électriques et magnétiques*

[6] CEI 60050-111:1996, Vocabulaire Electrotechnique International – Partie 111: Physique et chimie
Amendement 1 (2005)

[7] CEI 60050-351:2006, *Vocabulaire Electrotechnique International – Partie 351: Technologie de commande et de régulation*

[8] CEI 61508-4:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*[3]

[9] CEI 61508-1:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

[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 Modeling Using Petri Nets*, IEEE Transactions on Reliability Vol 44, no 3

[12] SIGNORET, J.-P., *Modelling the behavior 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

---

3 Le terme « module » (définition 3.3) n'apparaît plus dans la dernière édition.

[19] CEI 61165:2006, *Application des techniques de Markov*

[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 modeling and analysis with stochastical Petri nets* developed at the Institute for Traffic Safety and Automation Engineering of the Technical University of Braunschweig

Références non citées

CEI 60812:2006, *Techniques d'analyse de la fiabilité du système – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)*

CEI 61025:2006, *Analyse par arbre de panne (AAP)*

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

CEI 61511-3:2003, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 3: Conseils pour la détermination des niveaux exigés d'intégrité de sécurité*

CEI 61703:2001, *Expressions mathématiques pour les termes de fiabilité, de disponibilité, de maintenabilité et de logistique de maintenance*

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 modeling 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, 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 modeling 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

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch