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 62551:2012

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It also gives information on projects, replaced and withdrawn publications.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

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

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

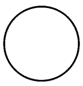
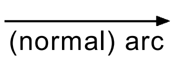
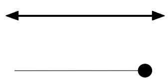
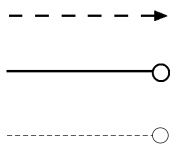
identifier 	*identifier*	*identifier*  *(weight)*	*n*  (normal) arc			
Place symbol, also used for multiple places	Transition symbol	Transition symbol with a transition weight	Relation symbols – normal arcs	Relation symbols – test arcs	Relation symbols – inhibitor arcs	Token symbol
There are various possibilities to draw test- and inhibitor-arcs. The token symbol is not a symbol of the static structure of the net but is used to symbolize the flow of information.						

Table 2 – Additional symbols in timed Petri nets

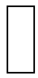
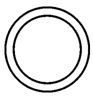
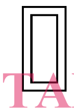
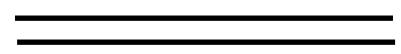
	Type of transition			
	Deterministic		**Stochastic**	
	Delay is zero	Delay is *d*	Exponentially or geometrically distributed	Arbitrarily distributed
Parameter		*d*	λ	$\varnothing$ Arbitrary distribution
Symbol				
NOTE In case of deterministic transitions, a Dirac distribution is often used. Furthermore, 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.

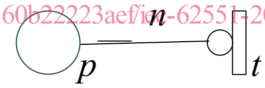
4.4.1 Further representations of Petri net elements

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.



IEC 1724/12

Figure 1 – Weighted inhibitor arc

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

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

4.4.1.3 Multiple places

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