This is a free page sample. Access the full version online.



Irish Standard I.S. EN 62551:2012

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

 $\label{eq:centre} @ \mbox{CENELEC 2012} & \mbox{No copying without NSAI permission except as permitted by copyright law}.$

Incorporating amendments/corrigenda issued since publication:

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard – national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation - recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

<i>This document replaces:</i>	<i>This document is base</i> EN 62551:2012	ed on: Pub 16 I	o <i>lished:</i> November, 2012
This document was published under the authority of the NSAI and comes into effect on: 19 November, 2012			
NSAI T +353 1 807 3800 Sales: 1 Swift Square, F +353 1 807 3838 T +353 1 85 Northwood, Santry E standards@nsai.ie F +353 1 85 Dublin 9 W NSAI.ie		ales: +353 1 857 67 +353 1 857 67 / standards.ie	'30 '29
Údarás um Chaighdeáin Náisiúnta na hÉireann			

EUROPEAN STANDARD

EN 62551

NORME EUROPÉENNE EUROPÄISCHE NORM

November 2012

ICS 21.020

English version

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

Techniques d'analyse de sûreté de fonctionnement -Techniques des réseaux de Petri (CEI 62551:2012) Analysemethoden für Zuverlässigkeit -Petrinetze (IEC 62551:2012)

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

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

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

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

CENELEC

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

Management Centre: Avenue Marnix 17, B - 1000 Brussels

© 2012 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.

EN 62551:2012

I.S. EN 62551:2012 - 2 -

Foreword

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

The following dates are fixed:

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

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

Endorsement notice

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

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

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

I.S. EN 62551:2012 - 3 -

EN 62551:2012

Annex ZA

(normative)

Normative references to international publications with their corresponding European publications

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

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

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

This page is intentionally left BLANK.

62551 © IEC:2012

CONTENTS

- 2 -

FO	FOREWORD				
INT	INTRODUCTION				
1	I Scope				
2	Norm	ative re	ferences	8	
3	Term	s, defin	itions, symbols and abbreviations	8	
	3.1	Terms	and definitions	8	
	3.2	Symbo	Is and abbreviations	10	
4	Gene	eral desc	cription of Petri nets	12	
	4.1	Untime	d low-level Petri nets	12	
	4.2	Timed	low-level Petri nets	12	
	4.3	High-le	evel Petri nets	13	
	4.4	Extens	ions of Petri nets and modelling with Petri nets	13	
		4.4.1	Further representations of Petri net elements	13	
F	Datri	4.4.2	Relationship to the concepts of dependability	14	
5	Petri		endability modeling and analysis	15	
	5.1 5.2	The ste	eps to be performed in general	15	
	5.2	5 2 1	General	10	
		522	Description of main parts and functions of the system (Step 1)	10	
		5.2.3	Modelling the structure of the system on the basis of Petri net-		
			submodels and their relations (Step 2)	16	
		5.2.4	Refining the models of Step 2 until the required level of detail is achieved (Step 3)	18	
		5.2.5	Analysing the model to achieve the results of interest (Step 4)	18	
		5.2.6	Representation and interpretation of results of analyses (Step 5)	19	
		5.2.7	Summary of documentation (Step 6)	20	
6	Relat	ionship	to other dependability models	20	
Anr	Annex A (informative) Structure and dynamics of Petri nets				
Anr	Annex B (informative) Availability with redundancy m-out-of-n				
Anr	Annex C (informative) Abstract example				
Anr	Annex D (informative) Modelling typical dependability concepts				
Anr	Annex E (informative) Level-crossing example				
Bib	Bibliography				
				4.0	
Figi	ure 1	– weigh		13	
Figi	ure 2	- Place	<i>p</i> is a multiple place	14	
Fig	ure 3	– Markir	ng on p after firing of transition t	14	
Fig	ure 4	– The a	ctivation of t depends on the value of V	14	
Fig	ure 5	- Metho	dology consisting mainly of 'modelling', 'analysing' and 'representing'	15	
Eigure 6 Dreeses for dependebility modelling and englysing with Data and					
Figi	Figure 5 – Frocess for dependability modelling and analysing with Feth field located located with				
mo	dels fo	or their f	functions and dependability	17	
Fig	ure 8	– Indica	tion of the analysis method as a function of the PN model	19	

62551 © IEC:2012

- 3 -

Figure A.1 – Availability state-transition circle of a component. 22 Figure A.2 – Transition 'failure' is enabled 23 Figure A.3 – 'Faulty' place marked due to firing of 'failure' 23 Figure A.5 – The token at the 'maintenance crew available' location is not used 24 Figure A.6 – Transition is not enabled 25 Figure A.6 – Marking before firing 25 Figure A.9 – PN with initial marking 25 Figure A.10 – Corresponding RG 25 Figure A.10 – Corresponding RG 26 Figure A.12 – Marking after firing of transition 'complor peair' 27 Figure A.12 – Marking after firing of transition 'complor peair' 27 Figure A.13 – A timed PN with two exponentially distributed timed transitions 28 Figure A.14 – The corresponding stochastic reachability graph 28 Figure B.1 – Two individual item availability nets with specific failure- and repair-rates 33 Figure B.2 – Stochastic reachability graph corresponding to Figure B.1 with global states (as an abbreviation c_1 is used for 'compl faulty') 34 Figure B.4 – Stochastic reachability graph corresponding to Figure B.3 with global states (as an abbreviation c_1 is used for 'compl faulty') 34 Figure B.4 – Stochastic reachability graph corresponding to Figure B.3 with global states 35<		
Figure A.2 - Transition 'failure' is enabled23Figure A.3 - 'Faulty' place marked due to firing of 'failure'23Figure A.4 - Transition 'comp1 repair' is enabled24Figure A.5 - The token at the 'maintenance crew available' location is not used24Figure A.6 - Transition is not enabled.25Figure A.7 - Marking before firing25Figure A.9 - PN with initial marking25Figure A.9 - PN with initial marking25Figure A.10 - Corresponding RG26Figure A.11 - Transitions 'comp1 repair' and 'comphp failure' are enabled26Figure A.12 - Marking after firing of transition 'comp1 repair'.27Figure A.13 - A timed PN with two exponentially distributed timed transitions.28Figure A.14 - The corresponding stochastic reachability graph.28Figure A.15 - Petri net with timed transitions29Figure B.1 - Two individual item availability nets with specific failure- and repair-rates33Figure B.2 - Stochastic reachability graph corresponding to Figure B.1 with global31states (as an abbreviation c_1 is used for 'comp1 faulty')33Figure B.4 - Stochastic reachability graph corresponding to Figure B.3 with globalstates (as an abbreviation c_1 is used for 'comp1 faulty')34Figure B.4 - Stochastic reachability graph corresponding to Figure B.335Figure B.4 - Stochastic reachability graph corresponding to Figure B.336Figure B.5 - Specifically connected 2-out-of-3 availability net35Figure B.4 - Stochastic reachability graph corresponding to Figure B.337 <tr< td=""><td>Figure A.1 – Availability state-transition circle of a component</td><td>22</td></tr<>	Figure A.1 – Availability state-transition circle of a component	22
Figure A.3 – 'Faulty' place marked due to firing of 'failure'23Figure A.4 – Transition 'comp1 repair' is enabled.24Figure A.5 – The token at the 'maintenance crew available' location is not used.24Figure A.6 – Transition is not enabled.25Figure A.7 – Marking before firing.25Figure A.7 – Marking after firing25Figure A.10 – Corresponding RG.25Figure A.10 – Corresponding RG.26Figure A.11 – Transitions 'comp1 repair' and 'comp1p repair'.27Figure A.12 – Marking after firing of transition 'comp1p repair'.27Figure A.13 – A timed PN with two exponentially distributed timed transitions.28Figure A.15 – Petri net with timed transitions28Figure B.1 – Two individual item availability nets with specific failure- and repair-rates33Figure B.2 – Stochastic reachability graph corresponding to Figure B.1 with global states (as an abbreviation c_1 is used for 'comp1 faulty').34Figure B.3 – Three individual item availability nets with specific failure rates and repair rates.33Figure B.4 – Stochastic reachability graph corresponding to Figure B.3 with global states (as an abbreviation c_1 is used for 'comp1 faulty').34Figure B.5 – Specifically connected 1-out-of-3 availability net.35Figure B.7 – Specifically connected 1-out-of-3 reliability net.36Figure B.9 – Specifically connected 2-out-of-3 reliability net.37Figure B.1 – Reachability graph for the net in Figure B.137Figure B.1 – Specifically connected 2-out-of-3 reliability net.37Figure B.1 – Reachabilit	Figure A.2 – Transition 'failure' is enabled	23
Figure A.4 – Transition 'comp1 repair' is enabled.24Figure A.5 – The token at the 'maintenance crew available' location is not used24Figure A.6 – Transition is not enabled.25Figure A.7 – Marking before firing25Figure A.9 – PN with initial marking25Figure A.10 – Corresponding RG25Figure A.11 – Transitions 'comp1p repair' and 'comphp failure' are enabled26Figure A.12 – Marking after firing of transition 'comp1p repair'27Figure A.13 – A timed PN with two exponentially distributed timed transitions.28Figure A.14 – The corresponding stochastic reachability graph28Figure B.2 – Detri net with timed transitions29Figure B.2 – Stochastic reachability graph corresponding to Figure B.1 – Two individual item availability nets with specific failure- and repair-rates33Figure B.3 – Three individual item availability nets with specific failure rates and repair rates33Figure B.4 – Stochastic reachability graph corresponding to Figure B.3 with global states (as an abbreviation c_1 is used for 'comp1 faulty')34Figure B.5 – Specifically connected 1-out-of-3 availability net35Figure B.5 – Specifically connected 2-out-of-3 availability net36Figure B.7 – Specifically connected 1-out-of-3 reliability net37Figure B.8 – Stochastic reachability graph for the net in Figure B.137Figure B.10 – Reachability graph for the net in Figure B.137Figure B.10 – Reachability graph for the net in Figure B.137Figure B.11 – Specifically connected 2-out-of-3 reliability net37Figur	Figure A.3 – 'Faulty' place marked due to firing of 'failure'	23
Figure A.5 – The token at the 'maintenance crew available' location is not used.24Figure A.6 – Transition is not enabled.25Figure A.7 – Marking before firing25Figure A.9 – PN with initial marking25Figure A.10 – Corresponding RG25Figure A.11 – Transitions 'complp repair' and 'comphp failure' are enabled26Figure A.12 – Marking after firing of transition 'comphp repair'.27Figure A.13 – A timed PN with two exponentially distributed timed transitions.28Figure A.14 – The corresponding stochastic reachability graph28Figure B.1 – Two individual item availability nets with specific failure- and repair-rates33Figure B.1 – Two individual item availability nets with specific failure and repair-rates33Figure B.3 – Three individual item availability nets with specific failure rates and repair33Figure B.4 – Stochastic reachability graph corresponding to Figure B.3 with global33Figure B.5 – Specifically connected 1-out-of-3 availability net35Figure B.5 – Specifically connected 2-out-of-3 availability net36Figure B.6 – Specifically connected 2-out-of-3 availability net37Figure B.1 – Reachability graph with system specific operating states36Figure B.1 – Specifically connected 2-out-of-3 reliability net37Figure B.1 – Specifically connected 2-out-of-3 reliability net <td>Figure A.4 – Transition 'comp₁ repair' is enabled</td> <td>24</td>	Figure A.4 – Transition 'comp ₁ repair' is enabled	24
Figure A.6 - Transition is not enabled.25Figure A.7 - Marking before firing.25Figure A.8 - Marking after firing.25Figure A.9 - PN with initial marking.25Figure A.10 - Corresponding RG25Figure A.11 - Transitions 'complp repair' and 'complp fepair'.27Figure A.12 - Marking after firing of transition 'complp repair'.27Figure A.13 - A timed PN with two exponentially distributed timed transitions.28Figure A.15 - Petri net with timed transitions.29Figure B.1 - Two individual item availability nets with specific failure- and repair-rates.33Figure B.2 - Stochastic reachability graph corresponding to Figure B.1 with globalstates (as an abbreviation $\overline{c_1}$ is used for 'comp1 faulty').33Figure B.3 - Three individual item availability nets with specific failure rates and repair rates.33Figure B.4 - Stochastic reachability graph corresponding to Figure B.3 with globalstates (as an abbreviation $\overline{c_1}$ is used for 'comp1 faulty')34Figure B.4 - Stochastic reachability graph corresponding to Figure B.3 with globalstates (as an abbreviation $\overline{c_1}$ is used for 'comp1 faulty')34Figure B.5 - Specifically connected 1-out-of-3 availability net35Figure B.7 - Specifically connected 1-out-of-3 availability net37Figure B.8 - Stochastic reachability graph for the net in Figure B.937Figure B.10 - Reachability graph for the net in Figure B.1137Figure B.12 - Reachability graph for the net in Figure B.1338Figure B.14 - Reachability graph for the net in Figure B.13.	Figure A.5 – The token at the 'maintenance crew available' location is not used	24
Figure A.7 – Marking before firing 25 Figure A.8 – Marking after firing 25 Figure A.9 – PN with initial marking 25 Figure A.10 – Corresponding RG 25 Figure A.11 – Transitions 'complp repair' and 'complp failure' are enabled 26 Figure A.12 – Marking after firing of transition 'complp repair' 27 Figure A.13 – A timed PN with two exponentially distributed timed transitions 28 Figure A.14 – The corresponding stochastic reachability graph 28 Figure B.1 – Two individual item availability nets with specific failure- and repair-rates 33 Figure B.1 – Two individual item availability nets with specific failure rates and repair rates 33 Figure B.3 – Three individual item availability nets with specific failure rates and repair rates 33 Figure B.4 – Stochastic reachability graph corresponding to Figure B.3 with global states (as an abbreviation $\overline{c_1}$ is used for 'comp1 faulty') 34 Figure B.5 – Specifically connected 1-out-of-3 availability net 35 Figure B.7 – Specifically connected 1-out-of-3 availability net 36 Figure B.1 – Specifically connected 2-out-of-3 availability net 37 Figure B.1 – Specifically connected 2-out-of-3 availability net 37 Figure B.1 – Specifically connected 2-out-of-3 reliability net	Figure A.6 – Transition is not enabled	25
Figure A.8 – Marking after firing. 25 Figure A.9 – PN with initial marking. 25 Figure A.10 – Corresponding RG 25 Figure A.12 – Marking after firing of transition 'complp repair'. 27 Figure A.13 – A timed PN with two exponentially distributed timed transitions. 28 Figure A.13 – A timed PN with two exponentially distributed timed transitions. 28 Figure A.14 – The corresponding stochastic reachability graph. 28 Figure B.1 – Two individual item availability nets with specific failure- and repair-rates. 33 Figure B.3 – Three individual item availability nets with specific failure rates and repair rates. 33 Figure B.3 – Three individual item availability nets with specific failure rates and repair rates. 33 Figure B.4 – Stochastic reachability graph corresponding to Figure B.3 with global states (as an abbreviation $\overline{c_1}$ is used for 'comp1 faulty') 34 Figure B.5 – Specifically connected 1-out-of-3 availability net 35 Figure B.7 – Specifically connected 1-out-of-3 availability net 36 Figure B.8 – Stochastic reachability graph with system specific operating states 36 Figure B.10 – Reachability graph for the net in Figure B.1 37 Figure B.10 – Reachability graph for the net in Figure B.11 37 Figure B.13 – Specifically	Figure A.7 – Marking before firing	25
Figure A.9 – PN with initial marking 25 Figure A.10 – Corresponding RG 25 Figure A.11 – Transitions 'compl _p repair' and 'compl _p failure' are enabled 26 Figure A.12 – Marking after firing of transition 'compl _p repair' 27 Figure A.13 – A timed PN with two exponentially distributed timed transitions 28 Figure A.14 – The corresponding stochastic reachability graph 28 Figure A.15 – Petri net with timed transitions 29 Figure B.1 – Two individual item availability nets with specific failure- and repair-rates 33 Figure B.2 – Stochastic reachability graph corresponding to Figure B.1 with global states (as an abbreviation \bar{c}_1 is used for 'comp1 faulty') 33 Figure B.4 – Stochastic reachability graph corresponding to Figure B.3 with global states (as an abbreviation \bar{c}_1 is used for 'comp1 faulty') 34 Figure B.5 – Specifically connected 1-out-of-3 availability net 35 Figure B.6 – Specifically connected 1-out-of-3 availability net 36 Figure B.7 – Specifically connected 1-out-of-3 availability net 37 Figure B.9 – Specifically connected 1-out-of-3 reliability net 37 Figure B.1 – Reachability graph for the net in Figure B.9 37 Figure B.1 – Reachability graph for the net in Figure B.1 37 Figure B.14 – Reachability	Figure A.8 – Marking after firing	25
Figure A.10 - Corresponding RG25Figure A.11 - Transitions 'complp repair' and 'comphp failure' are enabled26Figure A.12 - Marking after firing of transition 'complp repair'27Figure A.13 - A timed PN with two exponentially distributed timed transitions28Figure A.15 - Detri net with timed transitions29Figure B.1 - Two individual item availability nets with specific failure- and repair-rates33Figure B.2 - Stochastic reachability graph corresponding to Figure B.1 with global33Figure B.3 - Three individual item availability nets with specific failure rates and repair33Figure B.4 - Stochastic reachability graph corresponding to Figure B.3 with global33Figure B.4 - Stochastic reachability graph corresponding to Figure B.3 with global34states (as an abbreviation $\overline{c_1}$ is used for 'comp1 faulty')34Figure B.5 - Specifically connected 1-out-of-3 availability net35Figure B.6 - Specifically connected 3-out-of-3 availability net36Figure B.7 - Specifically connected 1-out-of-3 availability net36Figure B.9 - Specifically connected 2-out-of-3 reliability net37Figure B.10 - Reachability graph for the net in Figure B.937Figure B.11 - Specifically connected 2-out-of-3 reliability net38Figure B.12 - Reachability graph for the net in Figure B.1137Figure B.14 - Reachability graph for the net in Figure B.1338Figure B.14 - Reachability graph for the net in Figure C.1 with its global statesand aggregated global states according to availability and safety39Figure C.2 - S	Figure A.9 – PN with initial marking	25
Figure A.11 - Transitions 'complp repair' and 'comphp failure' are enabled26Figure A.12 - Marking after firing of transition 'complp repair'27Figure A.13 - A timed PN with two exponentially distributed timed transitions28Figure A.14 - The corresponding stochastic reachability graph28Figure A.15 - Petri net with timed transitions29Figure B.1 - Two individual item availability nets with specific failure- and repair-rates33Figure B.2 - Stochastic reachability graph corresponding to Figure B.1 with global33Figure B.3 - Three individual item availability nets with specific failure rates and repair rates33Figure B.4 - Stochastic reachability graph corresponding to Figure B.3 with global states (as an abbreviation c_1 is used for 'comp1 faulty')34Figure B.5 - Specifically connected 1-out-of-3 availability net35Figure B.6 - Specifically connected 2-out-of-3 availability net36Figure B.7 - Specifically connected 1-out-of-3 reliability net37Figure B.8 - Stochastic reachability graph with system specific operating states36Figure B.9 - Specifically connected 2-out-of-3 reliability net37Figure B.10 - Reachability graph for the net in Figure B.937Figure B.11 - Specifically connected 2-out-of-3 reliability net37Figure B.12 - Reachability graph for the net in Figure B.1338Figure B.13 - Specifically connected 2-out-of-3 reliability net37Figure B.14 - Reachability graph for the net in Figure B.1338Figure C.2 - Stochastic availability net37 <trr>Figure B.14 - Reachability graph f</trr>	Figure A.10 – Corresponding RG	25
Figure A.12 – Marking after firing of transition 'comple repair'	Figure A.11 – Transitions 'complo repair' and 'compho failure' are enabled	26
Figure A.13 – A timed PN with two exponentially distributed timed transitions.28Figure A.14 – The corresponding stochastic reachability graph28Figure A.15 – Petri net with timed transitions29Figure B.1 – Two individual item availability nets with specific failure- and repair-rates33Figure B.2 – Stochastic reachability graph corresponding to Figure B.1 with global33Figure B.3 – Three individual item availability nets with specific failure rates and repair33Figure B.4 – Stochastic reachability graph corresponding to Figure B.3 with global34states (as an abbreviation \bar{c}_1 is used for 'comp1 faulty')34Figure B.5 – Specifically connected 1-out-of-3 availability net35Figure B.6 – Specifically connected 2-out-of-3 availability net36Figure B.7 – Specifically connected 3-out-of-3 availability net36Figure B.9 – Specifically connected 1-out-of-3 reliability net37Figure B.10 – Reachability graph for the net in Figure B.937Figure B.11 – Specifically connected 2-out-of-3 reliability net37Figure B.12 – Reachability graph for the net in Figure B.1137Figure B.13 – Specifically connected 3-out-of-3 reliability net38Figure C.1 – Individual availability net39Figure C.3 – Basic reliability graph of the net in Figure B.1338Figure C.4 – General hierarchical net with supertransitions and superplaces41Figure C.5 – General hierarchical net with supertransitions and superplaces41Figure C.4 – General hierarchical net with supertransitions and superplaces42Figure	Figure A.12 – Marking after firing of transition 'completer repair'	27
Figure A.14 - The corresponding stochastic reachability graph28Figure A.15 - Petri net with timed transitions29Figure B.1 - Two individual item availability nets with specific failure- and repair-rates33Figure B.2 - Stochastic reachability graph corresponding to Figure B.1 with globalstates (as an abbreviation $\overline{c_1}$ is used for "comp1 faulty")	Figure A.13 – A timed PN with two exponentially distributed timed transitions	28
Figure A.15 – Petri net with timed transitions29Figure B.1 – Two individual item availability nets with specific failure- and repair-rates33Figure B.2 – Stochastic reachability graph corresponding to Figure B.1 with global states (as an abbreviation \bar{c}_1 is used for "comp1 faulty")33Figure B.3 – Three individual item availability nets with specific failure rates and repair rates33Figure B.4 – Stochastic reachability graph corresponding to Figure B.3 with global states (as an abbreviation \bar{c}_1 is used for 'comp1 faulty')34Figure B.5 – Specifically connected 1-out-of-3 availability net35Figure B.6 – Specifically connected 2-out-of-3 availability net36Figure B.7 – Specifically connected 3-out-of-3 availability net36Figure B.9 – Specifically connected 1-out-of-3 reliability net37Figure B.9 – Specifically connected 1-out-of-3 reliability net37Figure B.10 – Reachability graph for the net in Figure B.937Figure B.11 – Specifically connected 2-out-of-3 reliability net37Figure B.12 – Reachability graph for the net in Figure B.1137Figure B.14 – Reachability graph for the net in Figure B.1338Figure B.14 – Reachability graph for the net in Figure B.1338Figure C.2 – Stochastic availability net39Figure C.3 – Basic reliability and function modelling concept40Figure C.4 – General hierarchical net with supertransitions to model reliability41Figure C.5 – General hierarchical net with supertransitions to model availability41Figure C.6 – General hierarchical net with supertransitions and supe	Figure A.14 – The corresponding stochastic reachability graph	28
Figure B.1 – Two individual item availability nets with specific failure- and repair-rates	Figure A.15 – Petri net with timed transitions	29
Figure B.2 – Stochastic reachability graph corresponding to Figure B.1 with global states (as an abbreviation $\overline{c_1}$ is used for "comp1 faulty") 33 Figure B.3 – Three individual item availability nets with specific failure rates and repair 33 Figure B.4 – Stochastic reachability graph corresponding to Figure B.3 with global 34 states (as an abbreviation $\overline{c_1}$ is used for 'comp1 faulty') 34 Figure B.5 – Specifically connected 1-out-of-3 availability net 35 Figure B.6 – Specifically connected 2-out-of-3 availability net 36 Figure B.7 – Specifically connected 3-out-of-3 availability net 36 Figure B.8 – Stochastic reachability graph with system specific operating states 36 Figure B.9 – Specifically connected 2-out-of-3 reliability net 37 Figure B.10 – Reachability graph for the net in Figure B.9 37 Figure B.11 – Specifically connected 3-out-of-3 reliability net 38 Figure B.12 – Reachability graph for the net in Figure B.11 37 Figure B.13 – Specifically connected 3-out-of-3 reliability net 38 Figure C.1 – Individual availability net 39 Figure B.14 – Reachability graph for the net in Figure B.13 38 Figure C.3 – Basic reliability and function modelling concept 40 Figure C.4 – Gene	Figure B.1 – Two individual item availability nets with specific failure- and repair-rates	33
states (as an abbreviation $\overline{c_1}$ is used for "comp1 faulty")	Figure B.2 – Stochastic reachability graph corresponding to Figure B.1 with global	
Figure B.3 – Three individual item availability nets with specific failure rates and repair 33 Figure B.4 – Stochastic reachability graph corresponding to Figure B.3 with global 34 Figure B.5 – Specifically connected 1-out-of-3 availability net 35 Figure B.6 – Specifically connected 2-out-of-3 availability net 35 Figure B.7 – Specifically connected 3-out-of-3 availability net 36 Figure B.8 – Stochastic reachability graph with system specific operating states 36 Figure B.9 – Specifically connected 1-out-of-3 reliability net 37 Figure B.10 – Reachability graph for the net in Figure B.9 37 Figure B.11 – Specifically connected 2-out-of-3 reliability net 37 Figure B.12 – Reachability graph for the net in Figure B.11 37 Figure B.13 – Specifically connected 3-out-of-3 reliability net 38 Figure C.1 – Individual availability graph of the net in Figure B.13 38 Figure C.2 – Stochastic availability graph of the net in Figure C.1 with its global states 39 Figure C.4 – General hierarchical net with supertransitions to model reliability 41 Figure C.5 – General hierarchical net with supertransitions and superplaces 41 Figure C.4 – General hierarchical net with supertransitions and superplaces 42 Figure C.5 – General hierarchica	states (as an abbreviation $\overline{c_1}$ is used for "comp ₁ faulty")	33
rates 33 Figure B.4 – Stochastic reachability graph corresponding to Figure B.3 with global states (as an abbreviation \bar{c}_1 is used for 'comp ₁ faulty') 34 Figure B.5 – Specifically connected 1-out-of-3 availability net 35 Figure B.6 – Specifically connected 2-out-of-3 availability net 35 Figure B.7 – Specifically connected 3-out-of-3 availability net 36 Figure B.8 – Stochastic reachability graph with system specific operating states 36 Figure B.9 – Specifically connected 1-out-of-3 reliability net 37 Figure B.10 – Reachability graph for the net in Figure B.9 37 Figure B.11 – Specifically connected 2-out-of-3 reliability net 37 Figure B.12 – Reachability graph for the net in Figure B.11 37 Figure B.13 – Specifically connected 3-out-of-3 reliability net 38 Figure B.14 – Reachability graph for the net in Figure B.13 38 Figure C.1 – Individual availability net 39 Figure C.2 – Stochastic availability graph of the net in Figure C.1 with its global states and aggregated global states according to availability and safety 39 Figure C.3 – Basic reliability and function modelling concept 40 Figure C.4 – General hierarchical net with supertransitions and superplaces 41 Figure C.5 – General hierarchical net with supert	Figure B.3 – Three individual item availability nets with specific failure rates and repair	
Figure B.4 – Stochastic reachability graph corresponding to Figure B.3 with globalstates (as an abbreviation $\overline{c_1}$ is used for 'comp1 faulty')34Figure B.5 – Specifically connected 1-out-of-3 availability net35Figure B.6 – Specifically connected 2-out-of-3 availability net36Figure B.7 – Specifically connected 3-out-of-3 availability net36Figure B.8 – Stochastic reachability graph with system specific operating states36Figure B.9 – Specifically connected 1-out-of-3 reliability net37Figure B.10 – Reachability graph for the net in Figure B.937Figure B.11 – Specifically connected 2-out-of-3 reliability net37Figure B.12 – Reachability graph for the net in Figure B.1137Figure B.13 – Specifically connected 3-out-of-3 reliability net38Figure B.14 – Reachability graph for the net in Figure B.1338Figure B.14 – Reachability graph for the net in Figure B.1338Figure C.1 – Individual availability net39Figure C.2 – Stochastic availability graph of the net in Figure C.1 with its global statesand aggregated global states according to availability and safety40Figure C.5 – General hierarchical net with supertransitions to model reliability41Figure C.6 – General hierarchical net with supertransitions and superplaces42Figure E.1 – Applied example of a level crossing availability and superplaces42Figure E.2 – Main parts of the level crossing example model46Figure E.3 – Submodels of the level crossing example model47Figure E.4 – PN model of car and train traffic processes	rates	33
states (as an abbreviation c1 is used for 'comp1 faulty') 34 Figure B.5 – Specifically connected 1-out-of-3 availability net 35 Figure B.6 – Specifically connected 2-out-of-3 availability net 35 Figure B.7 – Specifically connected 3-out-of-3 availability net 36 Figure B.8 – Stochastic reachability graph with system specific operating states 36 Figure B.9 – Specifically connected 1-out-of-3 reliability net 37 Figure B.10 – Reachability graph for the net in Figure B.9 37 Figure B.11 – Specifically connected 2-out-of-3 reliability net 37 Figure B.12 – Reachability graph for the net in Figure B.11 37 Figure B.13 – Specifically connected 3-out-of-3 reliability net 38 Figure B.14 – Reachability graph for the net in Figure B.13 38 Figure C.1 – Individual availability net 39 Figure C.3 – Basic reliability and function modelling concept 40 Figure C.4 – General hierarchical net with supertransitions to model reliability 41 Figure C.5 – General hierarchical net with supertransitions and superplaces 42 Figure C.4 – General hierarchical net with supertransitions to model availability 41 Figure C.5 – General hierarchical net with supertransitions and superplaces 42 Figure C.4 –	Figure B.4 – Stochastic reachability graph corresponding to Figure B.3 with global	
Figure B.5 – Specifically connected 1-out-of-3 availability net 35 Figure B.6 – Specifically connected 2-out-of-3 availability net 35 Figure B.7 – Specifically connected 3-out-of-3 availability net 36 Figure B.8 – Stochastic reachability graph with system specific operating states 36 Figure B.9 – Specifically connected 1-out-of-3 reliability net 37 Figure B.10 – Reachability graph for the net in Figure B.9 37 Figure B.11 – Specifically connected 2-out-of-3 reliability net 37 Figure B.12 – Reachability graph for the net in Figure B.11 37 Figure B.13 – Specifically connected 3-out-of-3 reliability net 38 Figure B.14 – Reachability graph for the net in Figure B.13 38 Figure C.1 – Individual availability net 39 Figure C.2 – Stochastic availability graph of the net in Figure C.1 with its global states 39 Figure C.3 – Basic reliability and function modelling concept 40 Figure C.4 – General hierarchical net with supertransitions to model reliability 41 Figure C.5 – General hierarchical net with supertransitions and superplaces 41 Figure C.7 – General hierarchical net with supertransitions to model availability 41 Figure C.7 – General hierarchical net with supertransitions and superplaces 42 <td>states (as an abbreviation c_1 is used for 'comp₁ faulty')</td> <td>34</td>	states (as an abbreviation c_1 is used for 'comp ₁ faulty')	34
Figure B.6 – Specifically connected 2-out-of-3 availability net	Figure B.5 – Specifically connected 1-out-of-3 availability net	35
Figure B.7 – Specifically connected 3-out-of-3 availability net 36 Figure B.8 – Stochastic reachability graph with system specific operating states 36 Figure B.9 – Specifically connected 1-out-of-3 reliability net 37 Figure B.10 – Reachability graph for the net in Figure B.9 37 Figure B.11 – Specifically connected 2-out-of-3 reliability net 37 Figure B.12 – Reachability graph for the net in Figure B.11 37 Figure B.13 – Specifically connected 3-out-of-3 reliability net 38 Figure B.14 – Reachability graph for the net in Figure B.13 38 Figure C.1 – Individual availability net 39 Figure C.2 – Stochastic availability graph of the net in Figure C.1 with its global states 39 Figure C.3 – Basic reliability and function modelling concept 40 Figure C.4 – General hierarchical net with supertransitions to model reliability 41 Figure C.5 – General hierarchical net with supertransitions and superplaces 41 Figure C.7 – General hierarchical net with supertransitions and superplaces 42 Figure E.1 – Applied example of a level crossing and its protection system 45 Figure E.2 – Main parts of the level crossing example model 47 Figure E.4 – PN model of car and train traffic processes 48 <td>Figure B.6 – Specifically connected 2-out-of-3 availability net</td> <td>35</td>	Figure B.6 – Specifically connected 2-out-of-3 availability net	35
Figure B.8 – Stochastic reachability graph with system specific operating states 36 Figure B.9 – Specifically connected 1-out-of-3 reliability net 37 Figure B.10 – Reachability graph for the net in Figure B.9 37 Figure B.11 – Specifically connected 2-out-of-3 reliability net 37 Figure B.12 – Reachability graph for the net in Figure B.11 37 Figure B.13 – Specifically connected 3-out-of-3 reliability net 38 Figure B.14 – Reachability graph for the net in Figure B.13 38 Figure C.1 – Individual availability net 39 Figure C.2 – Stochastic availability graph of the net in Figure C.1 with its global states and aggregated global states according to availability and safety 39 Figure C.3 – Basic reliability and function modelling concept 40 Figure C.4 – General hierarchical net with supertransitions to model reliability 41 Figure C.5 – General hierarchical net with supertransitions to model availability 41 Figure C.6 – General hierarchical net with supertransitions and superplaces 42 Figure E.1 – Applied example of a level crossing and its protection system 45 Figure E.2 – Main parts of the level crossing example model 47 Figure E.3 – Submodels of the level crossing example model 47 Figure E.4 – PN model of car and train	Figure B.7 – Specifically connected 3-out-of-3 availability net	36
Figure B.9 – Specifically connected 1-out-of-3 reliability net 37 Figure B.10 – Reachability graph for the net in Figure B.9 37 Figure B.11 – Specifically connected 2-out-of-3 reliability net 37 Figure B.12 – Reachability graph for the net in Figure B.11 37 Figure B.13 – Specifically connected 3-out-of-3 reliability net 38 Figure B.14 – Reachability graph for the net in Figure B.13 38 Figure C.1 – Individual availability net 39 Figure C.2 – Stochastic availability graph of the net in Figure C.1 with its global states 39 Figure C.3 – Basic reliability and function modelling concept 40 Figure C.4 – General hierarchical net with supertransitions to model reliability 41 Figure C.5 – General hierarchical net with supertransitions and superplaces 41 Figure C.7 – General hierarchical net with supertransitions and superplaces 42 Figure E.1 – Applied example of a level crossing and its protection system 45 Figure E.2 – Main parts of the level crossing example model 47 Figure E.3 – Submodels of the level crossing example model 47 Figure E.4 – PN model of car and train traffic processes 48	Figure B.8 – Stochastic reachability graph with system specific operating states	36
Figure B.10 – Reachability graph for the net in Figure B.9 37 Figure B.11 – Specifically connected 2-out-of-3 reliability net 37 Figure B.12 – Reachability graph for the net in Figure B.11 37 Figure B.13 – Specifically connected 3-out-of-3 reliability net 38 Figure B.14 – Reachability graph for the net in Figure B.13 38 Figure C.1 – Individual availability net 39 Figure C.2 – Stochastic availability graph of the net in Figure C.1 with its global states and aggregated global states according to availability and safety 39 Figure C.3 – Basic reliability and function modelling concept 40 Figure C.5 – General hierarchical net with supertransitions to model reliability 41 Figure C.6 – General hierarchical net with supertransitions and superplaces 41 Figure C.7 – General hierarchical net with supertransitions and superplaces 42 Figure E.1 – Applied example of a level crossing and its protection system 45 Figure E.2 – Main parts of the level crossing example model 47 Figure E.3 – Submodels of the level crossing example model 47 Figure E.4 – PN model of car and train traffic processes 48	Figure B.9 – Specifically connected 1-out-of-3 reliability net	37
Figure B.11 – Specifically connected 2-out-of-3 reliability net 37 Figure B.12 – Reachability graph for the net in Figure B.11 37 Figure B.13 – Specifically connected 3-out-of-3 reliability net 38 Figure B.14 – Reachability graph for the net in Figure B.13 38 Figure C.1 – Individual availability net 39 Figure C.2 – Stochastic availability graph of the net in Figure C.1 with its global states 39 Figure C.3 – Basic reliability and function modelling concept 40 Figure C.4 – General hierarchical net with supertransitions to model reliability 41 Figure C.5 – General hierarchical net with supertransitions and superplaces 41 Figure C.7 – General hierarchical net with supertransitions to model availability 41 Figure C.7 – General hierarchical net with supertransitions and superplaces 42 Figure E.1 – Applied example of a level crossing and its protection system 45 Figure E.2 – Main parts of the level crossing example model 46 Figure E.3 – Submodels of the level crossing example model 47 Figure E.4 – PN model of car and train traffic processes 48	Figure B.10 – Reachability graph for the net in Figure B.9	37
Figure B.12 – Reachability graph for the net in Figure B.11 37 Figure B.13 – Specifically connected 3-out-of-3 reliability net 38 Figure B.14 – Reachability graph for the net in Figure B.13 38 Figure C.1 – Individual availability net 39 Figure C.2 – Stochastic availability graph of the net in Figure C.1 with its global states and aggregated global states according to availability and safety 39 Figure C.3 – Basic reliability and function modelling concept 40 Figure C.4 – General hierarchical net with supertransitions to model reliability 41 Figure C.5 – General hierarchical net with supertransitions and superplaces 41 Figure C.6 – General hierarchical net with supertransitions and superplaces 42 Figure E.1 – Applied example of a level crossing and its protection system 45 Figure E.2 – Main parts of the level crossing example model 46 Figure E.3 – Submodels of the level crossing example model 47 Figure E.4 – PN model of car and train traffic processes 48	Figure B.11 – Specifically connected 2-out-of-3 reliability net	37
Figure B.13 – Specifically connected 3-out-of-3 reliability net	Figure B.12 – Reachability graph for the net in Figure B.11	37
Figure B.14 – Reachability graph for the net in Figure B.13	Figure B.13 – Specifically connected 3-out-of-3 reliability net	38
Figure C.1 – Individual availability net.39Figure C.2 – Stochastic availability graph of the net in Figure C.1 with its global states39and aggregated global states according to availability and safety39Figure C.3 – Basic reliability and function modelling concept40Figure C.4 – General hierarchical net with supertransitions to model reliability41Figure C.5 – General hierarchical net with supertransitions and superplaces41Figure C.6 – General hierarchical net with supertransitions to model availability41Figure C.7 – General hierarchical net with supertransitions and superplaces42Figure E.1 – Applied example of a level crossing and its protection system45Figure E.2 – Main parts of the level crossing example model46Figure E.3 – Submodels of the level crossing example model47Figure E.4 – PN model of car and train traffic processes48	Figure B.14 – Reachability graph for the net in Figure B.13	38
Figure C.2 – Stochastic availability graph of the net in Figure C.1 with its global states 39 Figure C.3 – Basic reliability and function modelling concept 40 Figure C.4 – General hierarchical net with supertransitions to model reliability 41 Figure C.5 – General hierarchical net with supertransitions and superplaces 41 Figure C.6 – General hierarchical net with supertransitions to model availability 41 Figure C.7 – General hierarchical net with supertransitions and superplaces 42 Figure E.1 – Applied example of a level crossing and its protection system 45 Figure E.2 – Main parts of the level crossing example model 46 Figure E.3 – Submodels of the level crossing example model 47 Figure E.4 – PN model of car and train traffic processes 48	Figure C.1 – Individual availability net	39
and aggregated global states according to availability and safety39Figure C.3 – Basic reliability and function modelling concept40Figure C.4 – General hierarchical net with supertransitions to model reliability41Figure C.5 – General hierarchical net with supertransitions and superplaces41Figure C.6 – General hierarchical net with supertransitions to model availability41Figure C.7 – General hierarchical net with supertransitions and superplaces42Figure E.1 – Applied example of a level crossing and its protection system45Figure E.2 – Main parts of the level crossing example model46Figure E.3 – Submodels of the level crossing example model47Figure E 4 – PN model of car and train traffic processes48	Figure C.2 – Stochastic availability graph of the net in Figure C.1 with its global states	
Figure C.3 – Basic reliability and function modelling concept40Figure C.4 – General hierarchical net with supertransitions to model reliability41Figure C.5 – General hierarchical net with supertransitions and superplaces41Figure C.6 – General hierarchical net with supertransitions to model availability41Figure C.7 – General hierarchical net with supertransitions and superplaces42Figure E.1 – Applied example of a level crossing and its protection system45Figure E.2 – Main parts of the level crossing example model46Figure E.3 – Submodels of the level crossing example model47Figure E 4 – PN model of car and train traffic processes48	and aggregated global states according to availability and safety	39
Figure C.4 – General hierarchical net with supertransitions to model reliability	Figure C.3 – Basic reliability and function modelling concept	40
Figure C.5 – General hierarchical net with supertransitions and superplaces41Figure C.6 – General hierarchical net with supertransitions to model availability41Figure C.7 – General hierarchical net with supertransitions and superplaces42Figure E.1 – Applied example of a level crossing and its protection system45Figure E.2 – Main parts of the level crossing example model46Figure E.3 – Submodels of the level crossing example model47Figure E 4 – PN model of car and train traffic processes48	Figure C.4 – General hierarchical net with supertransitions to model reliability	41
Figure C.6 – General hierarchical net with supertransitions to model availability41Figure C.7 – General hierarchical net with supertransitions and superplaces42Figure E.1 – Applied example of a level crossing and its protection system45Figure E.2 – Main parts of the level crossing example model46Figure E.3 – Submodels of the level crossing example model47Figure E 4 – PN model of car and train traffic processes48	Figure C.5 – General hierarchical net with supertransitions and superplaces	41
Figure C.7 – General hierarchical net with supertransitions and superplaces 42 Figure E.1 – Applied example of a level crossing and its protection system 45 Figure E.2 – Main parts of the level crossing example model 46 Figure E.3 – Submodels of the level crossing example model 47 Figure E 4 – PN model of car and train traffic processes 48	Figure C.6 – General hierarchical net with supertransitions to model availability	41
Figure E.1 – Applied example of a level crossing and its protection system 45 Figure E.2 – Main parts of the level crossing example model 46 Figure E.3 – Submodels of the level crossing example model 47 Figure E 4 – PN model of car and train traffic processes 48	Figure C.7 – General hierarchical net with supertransitions and superplaces	42
Figure E.2 – Main parts of the level crossing example model	Figure E.1 – Applied example of a level crossing and its protection system	45
Figure E.3 – Submodels of the level crossing example model	Figure E.2 – Main parts of the level crossing example model	46
Figure E 4 – PN model of car and train traffic processes 48	Figure E.3 – Submodels of the level crossing example model	47
	Figure E.4 – PN model of car and train traffic processes	48

- 4 -

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

62551 © IEC:2012

- 5 -

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.
- 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.

- 6 -

62551 © IEC:2012

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.

62551 © IEC:2012

- 7 -

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.

- 8 -

62551 © IEC:2012

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



This is a free preview. Purchase the entire publication at the link below:

Product Page

S Looking for additional Standards? Visit Intertek Inform Infostore

> Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation