
Abbildungsverzeichnis

2.1	Die Welt der Objekte	35
2.2	Ein Systemzustand	39
2.3	Eine Zustandsveränderung	40
2.4	Ein Verhalten	42
2.5	Eine nahe Veränderung	42
2.6	Eine entfernte Veränderung	42
2.7	Eine Referenzverhalten	43
2.8	Ein dem Referenzverhalten nahes Verhalten	43
2.9	Ein dem Referenzverhalten weiter entferntes Verhalten	43
2.10	Nähere und entferntere Verhalten	44
2.11	Alle Verhalten, angeordnet in „Entfernungskreisen“	45
2.12	Korrektes Schliessen auf Fehler mit falscher Prämisse	47
2.13	Korrektes Schliessen auf Fehler	48
2.14	Korrektes Schliessen auf Fehler, 2	49
3.1	The Warsaw WB-Graph: overall pattern	64
3.2	The Warsaw WB-Graph, lower part	65
3.3	The Warsaw WB-Graph, middle part	66
3.4	The Warsaw WB-Graph, upper part	67
3.5	The Habsheim WB-Graph	69
4.1	Initialer Why-Because-Graph	78
4.2	Finaler Why-Because-Graph	79
4.3	Editierter Why-Because-Graph	89
4.4	Resultierender Why-Because-Graph	99

5.1	Das Beispielsystem, Zustands-Aktionsdiagramm mit Wahrscheinlichkeiten, Hazards und Zielen.	111
5.2	Zusammenfassung der Berechnungen	118
5.3	Hazardzustände für die Verschiedenen Auffassungen eines Hazards	121
8.1	Integrated Communication Bus System	160
8.2	epWBA of deviation „The Network has no Shielding“	163
8.3	NIC is not intact	164
8.4	Extend of Elements in System Description's Ontology	165
8.5	Expressible and Inexpressible Deviations	166
8.6	Resulting Fault Tree	168
8.7	epWBG formulated to describe deviation	169
8.8	Head of Fault Tree	169
9.1	A Communications Bus for Road Vehicle Electronics	175
10.1	Zusätzliche Sicherheitsaxiome auf Ebene 1	217
10.2	Schematische Zuggleitstrecke	219
10.3	Zustandsmaschine	221
10.4	Sicherheitsaxiome auf Ebene 2	225
10.5	Message Flow Graph	229
10.6	Beispiel einer Prozedur-Spezifikation in SPARK	230
10.7	Prozeduren für Zugführer	231
10.8	Beispiel eines Include-Files für den Model-Checkers	239
10.9	Reduzierte Zustandsmaschine des PROMELA-Prozesses für den Zugführer	240
10.10	Reduzierte Zustandsmaschine des PROMELA-Prozesses für den Zuggleiter	241
10.11	Ausgabe eines SPIN-Verifier-Durchlaufs	243
10.12	Beziehungen zwischen Message-Flow-Graph, SPARK Code und Promela-Modell	251
12.4	A Simple „Waterfall“ Model of Software Development	271
12.1	Lifecycle according to IEC 61508	274
12.2	E/E/PES Safety-Lifecycle	275
12.3	Software Safety Lifecycle	276
12.5	Level crossing Photo Mark Kobayashi-Hillary	277
12.6	Determining Risk Reduction	281

12.7 ALARP	285
12.8 Deployed Thrust Reversers	293
12.9 Deployed Spoilers of an Airbus A319	295
12.10A „dead man’s handle“ on a suburban train	297
16.1 Zuverlässigkeitsfunktion R^{ign}	334
16.2 Zuverlässigkeits- R und Parameterfunktion $a(\cdot)$ (links) bzw. $b(\cdot)$ (rechts) ($T = 10^6, t_0 = 10^3$)	335

Tabellenverzeichnis

8.1	Objects of the System	159
8.2	Properties of NIC	159
8.3	Properties of Wiring	159
8.4	Properties of Transmission	159
8.5	Relations of the System	160
8.6	HAZOP guide-words used and their interpretations	161
9.1	Objects and Their Properties	179
9.2	Relations and Their Object Types	180
9.3	List of Hazardous Happenstances for Level 0, and Associated SafeReqs	191
9.4	Meaning Postulates for Level 0	191
9.5	Assumptions on which HazAn is based, Level 0	192
9.6	New Vocabulary to be Defined at Later Stages, Level 0	192
9.7	Partial List for Level 1, HazHapps and Ensuing Safety Requirements .	200
9.8	Partial List for Level 1, Identified HazHapps Retained for Processing Later	200
9.9	Partial List for Level 1, Already-identified HazHapps to be Analysed .	201
9.10	List for Level 1, New Object Types Introduced	202
9.11	List for Level 1, Meaning Postulates	202
9.12	List of assumptions Introduced at Level 1	202
9.13	List of New Primitives Introduced at Level 1	203
9.14	List for Level 2, New Entities Added	203
9.15	Partial List Level 2, HazHapps and Ensuing Safety Requirements . . .	203
9.16	Partial List Level 2, Identified HazHapps to be Analysed Later	204

9.17 Partial List of HazHapps With Safety Requirements at Levels up to and including 2	206
9.18 Partial List up to and including Level 2, HazHapps to be Analysed Later	206
9.19 List for Levels up to and Including Level 2, Meaning Postulates	207
9.20 List for Levels up to and Including Level 2, Assumptions	208
9.21 List for Levels up to and Including Level 2, New Vocabulary to be Defined Later	208
10.1 Sorten auf Ebene 0 („Level 0“)	212
10.2 Binäre Relationen auf Ebene 0	213
10.3 Sicherheitsaxiome der Ebene 0	214
10.4 Sorten auf Ebene 1 („Level 1“)	215
10.5 Binäre Relationen auf Ebene 1	216
10.6 Ternäre Relationen auf Ebene 1	216
10.7 Sorten auf Ebene 2	218
10.8 Binäre Relationen auf Ebene 2	219
10.9 Ternäre Relationen auf Ebene 2	220
10.10 Zustände des Automaten in Ebene 2	222
10.11 Beschreibung der Zustände in natürlicher Sprache	223
10.12 Liste aller möglichen Ausgangssituationen für 4 Züge und 5 Stationen	238
10.13 Liste der zu überprüfenden Ausgangssituationen für 4 Züge und 5 Stationen	242
10.14 Benötigte Ressourcen für die Verifikation	245
12.1 Safety Integrity Levels	288

Literaturverzeichnis

- [1] BARNES, J. : *High Integrity Software: The SPARK Approach to Safety and Security*. Addison Wesley, 2003. – ISBN 0–321–13616–0
- [2] BECK, U. : *Risikogesellschaft: Auf dem Weg in eine andere Moderne*. Frankfurt am Main : Suhrkamp Verlag, 1986
- [3] BEDFORD, T. ; COOKE, R. : *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge University Press, 2001
- [4] U.K. CIVIL AVIATION AUTHORITY: Interference levels in aircraft at radio frequencies used by portable telephones. / U.K. Civil Aviation Authority. Verfügbar unter <http://www.srg.caa.co.uk/srg/seg.news.asp>, May 2000 (9/40-23-90-02). – Forschungsbericht
- [5] CARNAP, R. : Meaning Postulates. In: *Philosophical Studies* 3 (1952), S. 65–73
- [6] DIJKSTRA, E. W.: Guarded commands, non-determinacy and formal derivation of programs. In: *Communications of the ACM* 18 (1975), Nr. 8, 453–457. <http://www.cs.utexas.edu/users/EWD/ewd04xx/EWD472.PDF>
- [7] DRISCOLL, K. ; HALL, B. ; SIVENCRONA, H. ; ZUMSTEG, P. : Byzantine Fault Tolerance, from Theory to Reality. In: *SAFECOMP*, 235-248
- [8] Det-Tronics University: *Det-Tronics to Feature Flame and Gas Detection Systems at the NFPA America's Fire & Security Expo*. <http://www.detrronics.com/utcfs/ws-462/Assets/NFPA%20Miami%20Press%20Release.pdf>. Version: July 2006
- [9] DUVAL, G. ; JULLIAND, J. : Modeling and Verification of the RUBIS μ -Kernel with SPIN. In: *Proceedings of the First SPIN Workshop*
- [10] Emerson Process Management: *Emerson's Fisher control valves are first to be*

- SIL 3 certified to IEC 61508 standards.* http://www.emersonprocess.com/home/news/pr/806_sil3valves.html. Version: June 2008
- [11] *Esterel-Technologies-Joins-the-Wind-River-Partner-Validation-Program.* <http://www.esterel-technologies.com/news-events/press-releases/2009/Esterel-Technologies-Joins-the-Wind-River-Partner-Validation-Program>
Version: October 2009
- [12] FISHER, F. A.: Some Notes on Sparks and Ignition of Fuels / NASA/Lightning Technologies Inc. Langley Research Center, Hampton, VA, March 2000. – Technical Report NASA/TM-2000-210077
- [13] GARLINGTON, K. E.: *Persönliche Unterhaltung.* Juni 1998
- [14] GNESI, S. ; LENZINI, G. ; LATELLA, D. ; ABBANEO, C. ; AMENDOLA, A. ; MARMO, P. : An Automatic SPIN Validation of a Safety Critical Railway Control System. In: *Proceedings of the 2000 International Conference on Dependable Systems and Networks*, 119–224
- [15] GREGOIRE, J. C.: State space compression in Spin with GETSs. In: *Proceedings of the Second Spin Workshop.* New Brunswick, New Jersey : American Mathematical Society, August 1996
- [16] Investigation Commission concerning the accidents which occurred on June 26th 1988 at Mulhouse-Habsheim (68) to the Airbus A320, registered F-GFKC. Final Report. 1989. – Accident Investigation Report
- [17] HAZELL, R. W. ; MCHATTIE, G. V. ; WRIGHTSON, I. : Note on Hazard and Operability Studies [HAZOP]. Piccadilly, London W1J 0BA : Burlington House, 2001. – Forschungsbericht
- [18] HENKEL, D. : *Safely Sliding Windows.* <http://www.rvs.uni-bielefeld.de/research/RLPver/ssw-full.ps.gz>. Version: Mai 1997
- [19] HOARE, C. A. R.: Communicating Sequential Processes. In: *Communications of the ACM* 21 (1978), Nr. 8, 666–677. <http://www.cs.virginia.edu/crab/hoare1978csp.pdf>
- [20] HOLZMANN, G. J.: The Engineering of a Model Checker: the Gnu i-Protocol Case Study Revisited / Bell Laboratories, Lucent Technologies. Version: 1999. <http://spinroot.com/spin/Doc/spin99.pdf>. – Forschungsbericht. – Elektronische Ressource

- [21] HOLZMANN, G. J.: *The SPIN Model Checker*. Addison Wesley, 2003. – ISBN 0-321-22862-6
- [22] HOLZMANN, G. J. ; PELED, D. : An improvement in formal verification. In: *Proceedings of the 7th IFIP WG6.1 International Conference on Formal Description Techniques VII*. London, UK, UK : Chapman & Hall, Ltd., 1995. – ISBN 0-412-64450-9, S. 197-211
- [23] HOLZMANN, G. J. ; SMITH, M. H.: Automating Software Feature Verification. In: *Bell Labs Technical Journal Special Issue on Software Complexity (2000)*, April-June. <http://spinroot.com/gerard/pdf/bltj2000.pdf>
- [24] HUME, D. : *An Enquiry Concerning Human Understanding*. 3. Hrsg. L.A. Selby-Bigge und P.H. Nidditch : Oxford University Press, 1777/1975
- [25] International Electrotechnical Commission: *International Standard 61882, Hazard and Operability studies, Application Guide*. First. May 2001
- [26] JERVIS, R. : *System Effects: Complexity in Political and Social Life*. New Jersey : Princeton University Press, 1997
- [27] KAMMEN, D. M. ; HASSENZAHL, D. M.: Should We Risk It? Exploring Environmental, Health, and Technological Problem Solving. In: *Health, and Technological Problem Solving*, Princeton University Press, 1999
- [28] KRANTZ, D. H. ; LUCE, R. D. ; SUPPES, P. ; TVERSKY, A. : *Foundations of Measurement, Volume 1: Additive and Polynominal Representations*. New York, London : Academic Press, 1971
- [29] KUMAMOTO, H. ; HENLEY, E. J.: Probabilistic Risk Assessment and Management for Engineers and Scientists. In: *Institute of Electrical and Electronics Engineers, Inc*, IEEE Press, 1996
- [30] LADKIN, P. : *Formal But Lively Buffers in TLA+*. <http://www.rvs.uni-bielefeld.de/publications/Papers/newbuffer.ps.gz>. Version: Jan. 1996
- [31] LADKIN, P. : On classification of factors in failures and accidents / RVS Group, Faculty of Technology, University of Bielefeld. 1999 (RVS-Occ-99-04, available through [35]). – Forschungsbericht
- [32] LADKIN, P. : Causal Reasoning about Aircraft Accidents. In: *In proceedings of SAFECOMP 2000 conference*, 2000, S. 344-360

- [33] LADKIN, P. : Notes on the foundations of system safety analysis / RVS Group, Faculty of Technology, University of Bielefeld. 2000 (RVS-Bk-00-01, available through [35]). – Forschungsbericht
- [34] LADKIN, P. ; LOER, K. : Why-Because Analysis: Formal Reasoning About Incidents / RVS Group, Faculty of Technology, University of Bielefeld. 1998 (RVS-Bk-98-01, available through [35]). – Forschungsbericht
- [35] LADKIN, P. ; RVS GROUP the: *Publikationen AG RVS*. Arbeitsgruppe Rechner-netze und Verteilte Systeme (RVS), Technische Fakultät, Universität Bielefeld, Verfügbar unter <http://www.rvs.uni-bielefeld.de/>,
- [36] LADKIN, P. B.: Ontological Analysis. In: *SafetySystems* 14 (2005), May, Nr. 3. [http://www.rvs.uni-bielefeld.de/\\\$\\rightarrow\\$Publications\\\$\\rightarrow\\$PublicationsofRecord](http://www.rvs.uni-bielefeld.de/\$\\rightarrow$Publications\$\\rightarrow$PublicationsofRecord)
- [37] LADKIN, P. B. ; LAMPORT, L. ; OLIVIER, B. ; ROEGEL, D. : Lazy Caching in TLA. In: *Distributed Computing* (1999), Nr. 12, 151–174. <http://www.rvs.uni-bielefeld.de/publications/abstracts.html#Lazy>
- [38] LADKIN, P. B. ; LEUE, S. : Interpreting Message Flow Graphs. In: *Formal Aspects of Computing* 7 (1995), Nr. 5, S. 473–509
- [39] LADKIN, P. B.: *Foundations of System Analysis, Chapter 3 of Causal System Analysis*. <http://www.rvs.uni-bielefeld.de/publications/books/ComputerSafetyBook/index.html>. Version: 2001
- [40] LADKIN, P. B.: An Overview of IEC 61508 on E/E/PE Functional Safety. Version: 2008. <http://www.causalis.com/IEC61508FunctionalSafety.pdf>. – Forschungsbericht. – Elektronische Ressource
- [41] LAMPORT, L. : How to write a long formula / DEC Systems Research Center. Version: 1994. <http://research.microsoft.com/en-us/um/people/lamport/pubs/lamport-howtowrite.pdf> (119). – Technical Report. – Elektronische Ressource
- [42] LAMPORT, L. : TLA in Pictures. In: *IEEE Transactions on Software Engineering* SE-21 (1995), September, 768-775. <http://research.microsoft.com/en-us/um/people/lamport/pubs/lamport-pictures.pdf>
- [43] LAPRIE, J.-C. (Hrsg.): *Dependability: Basic Concepts and Terminology, in English, French, German, Italian and Japanese*. Bd. 5 of Dependable Computing and Fault

- Tolerance, Prepared by IFIP Working Group 10.5 on *Dependable Computing and Fault Tolerance*. Wien, New York : Springer Verlag, 1992
- [44] LEVESON, N. G.: *Safeware: System Safety and Computers*. New York, NY, USA : ACM, 1995. – ISBN 0–201–11972–2
- [45] LEWIS, D. : Causation. In: *Journal of Philosophy* 70 (1973), S. 556–567
- [46] LEWIS, D. : *Counterfactuals*. Oxford University Press, Inc., Blackwell, 1973
- [47] LIN, S. ; COSTELLO, D. J.: *Error Control Coding*. 2. Prentice Hall <http://www.worldcat.org/isbn/0130426725>. – ISBN 0130426725
- [48] LITTLEWOOD, B. ; STRIGINI, L. : Validation of ultrahigh dependability for software-based systems. In: *Commun. ACM* 36 (1993), November, Nr. 11, 69–80. <http://dx.doi.org/10.1145/163359.163373>. – ISSN 0001–0782
- [49] LLOYD, E. ; TYE, W. : *Systematic Safety: Safety Assessment of Aircraft Systems*. London : Civil Aviation Authority, 1982
- [50] LUHMANN, N. : *Soziologie des Risikos*. Berlin, New York : Walter de Gruyter, 1991
- [51] MACKIE, J. : *The Cement of the Universe: A Study of Causation*. Oxford : Clarendon Press, 1991
- [52] MEULEN, M. van d.: *Definitions for Hardware and Software Safety Engineers*. Springer Verlag London Limited, 2000
- [53] MILL, J. S.: *A System of Logic, Books I-III, volume VII of Collected Works*. London: Routledge & Kegan Paul : University of Toronto Press, 1973
- [54] The NetBSD Foundation: *NetBSD Web Site*. <http://www.netbsd.org/>. Version: August 2011
- [55] PAPADOPOULOS, Y. ; LEVESON, N. u.a.: *On the Safety Level of a Valve*. <http://www.cs.york.ac.uk/hise/safety-critical-archive/2009/0885.html>. Version: October 2009
- [56] PARNAS, D. L.: On the criteria to be used in decomposing systems into modules. In: *Commun. ACM* 15 (1972), December, Nr. 12, 1053–1058. <http://dx.doi.org/10.1145/361598.361623>. – ISSN 0001–0782
- [57] PARSONS, T. : What is an Argument? In: *The Journal of Philosophy* 93 (1996), April, Nr. 4, 164–185. <http://www.humnet.ucla.edu/humnet/phil/faculty/tparsons/Argumentation/What%20is%20an>

%20argument.pdf

- [58] PERROW, C. : *Normal Accidents: Living with High-Risk Technologies*. New York : Basic Books, 1984
- [59] QUINE, W. V. O.: *From a Logical Point of View*. 2. Harvard University Press, 1965
- [60] REDMILL, F. ; CHUDLEIGH, M. ; CATMUR, J. : *System Safety : HAZOP and Software HAZOP*. John Wiley & Sons <http://www.worldcat.org/isbn/0471982806>. – ISBN 0471982806
- [61] SAGAN, S. D.: *The Limits of Safety: Organisations, Accidents and Nuclear Weapons*. New Jersey : Princeton University Press, 1993
- [62] SHRADER-FRECHETTE, K. : *Risk Analysis and Scientific Method*. Dordrecht, Netherlands : D. Reidel Publishing Company, 1985
- [63] SHRADER-FRECHETTE, K. : *Risk and Rationality*. Berkeley and Los Angeles, CA : University of California Press, 1991
- [64] SIEKER, B. : *Systemanforderungsanalyse von Bahnbetriebsverfahren mit Hilfe der Ontological Hazard Analysis am Beispiel des Zugleitbetriebs nach FV-NE*, Universität Bielefeld, Diss., 2010
- [65] STUPHORN, J. ; SIEKER, B. ; LADKIN, P. : Dependable Risk Analysis for Systems with E/E/PE Components: Two Case Studies. In: *Proceedings of the Safety-critical Systems Symposium 2009* (2009)
- [66] STUPHORN, J. : *Iterative Decomposition of a Communication-Bus System using Ontological Analysis*, Universität Bielefeld, Diplomarbeit, July 2005. – RVS-Dip-05-02 Online: <http://www.rvs.uni-bielefeld.de/> → Publications → Theses
- [67] SWAIM, R. L.: System Group Chairman's Factual Report of Investigation. Technical Report Docket SA-516, Exhibit 9A / National Transportation Safety Board. Washington, D.C., August 2000. – Forschungsbericht
- [68] TANENBAUM, A. S.: *Computer Networks (4th Edition)*. 4. Prentice Hall, 2002. – ISBN 0130661023
- [69] U.K. HEALTH AND SERVICE EXECUTIVE: Dispensing petrol as a fuel – health and safety guidance for employees. / U.K. Health and Service Executive. Verfügbar unter <http://www.hse.gov.uk/pubns/indg216.htm>, 1997 (C338 IND(G)216L 2/97). – Forschungsbericht

-
- [70] UNITED STATES AIR FORCE: *Air Force Instructions 91-204*. July 1994
- [71] Verband Deutscher Verkehrsunternehmen: *Fahrdienstvorschrift für Nichtbundes-eigene Eisenbahnen (FV-NE)*. 2004. 2004. – Ausgabe 1984, Fassung 2004
- [72] VESELY, W. E. ; GOLDBERG, F. F. ; ROBERTS, N. H. ; HAASL, D. F.: *Fault Tree Handbook*. Washington, DC : U.S. Nuclear Regulatory Commission, 1981
- [73] Report on the Accident to Airbus A320-211 Aircraft in Warsaw on 14 September 1993. 1993 (available through [35]). – Accident Investigation Report