Bibliography

[1] A. Elfes, J. L. Hall, J. F. Montgomery, C. F. Bergh, and B. A. Dudik, "Towards a substantionally autonomous aerobot for exploration of Titan," in *Proc. of the IEEE International Conference on Robotics and Automation*, pp. 2535–2541, 2004.

[2] J. W. Burdick, N. E. Du Toit, A. Howard, C. Looman, J. Ma, R. M. Murray, and T. Wongpiromsarn, "Sensing, navigation and reasoning technologies for the DARPA Urban Challenge," tech. rep., DARPA Urban Challenge Final Report, 2007.

[3] S. Croomes, "Overview of the DART Mishap Investigation Results," tech. rep., National Aeronautics and Space Administration, 2006.

[4] L. B. Cremean, T. B. Foote, J. H. Gillula, G. H. Hines, D. Kogan, K. L. Kriechbaum, J. C. Lamb, J. Leibs, L. Lindzey, A. D. Stewart, J. W. Burdick, and R. M. Murray, "Alice: An information-rich autonomous vehicle for high-speed desert navigation," *Journal of Field Robotics*, vol. 23, pp. 777–810, 2006.

[5] P. S. Morgan, "Fault protection techniques in JPL spacecraft," in *Proc. of the First International Forum on Integrated System Health Engineering and Management in Aerospace (ISHEM)*, 2005.

[6] E. M. Clarke and J. M. Wing, "Formal methods: State of the art and future directions," *ACM Computing Surveys*, vol. 28, no. 4, pp. 626–643, 1996.

[7] P. Abbeel, A. Coates, M. Montemerlo, A. Y. Ng, and S. Thrun, "Discriminative training of Kalman filters," in *Proc. of Robotics: Science and Systems*, 2005.

[8] P. Goel, G. Dedeoglu, S. I. Roumeliotis, and G. S. Sukhatme, "Fault detection and identification in a mobile robot using multiple model estimation and neural network," in *Proc. of the IEEE International Conference on Robotics and Automation*, pp. 2302–2309, 2000.

[9] M. W. Hofbaur and B. C. Williams, "Hybrid diagnosis with unknown behavioral modes," in *Proc. of the 13th International Workshop on Principles of Diagnosis*, 2002.

[10] V. Verma, G. Gordon, R. Simmons, and S. Thrun, "Real-time fault diagnosis [robot fault diagnosis]," *IEEE Robotics and Automation Magazine*, vol. 11, no. 2, pp. 56–66, 2004.

[11] K. Ben Lamine and F. Kabanza, "History checking of temporal fuzzy logic formulas for monitoring behavior-based mobile robots," in *Proc. of the 12th IEEE International Conference on Tools with Artificial Intelligence*, 2000.

[12] M. Blanke, M. Staroswiecki, and N. E. Wu, "Concepts and methods in fault-tolerant control," in *Proc. of the American Control Conference*, 2001.

[13] C. Ferrell, "Failure recognition and fault tolerance of an autonomous robot," *Adaptive Behaviour*, vol. 2, no. 4, pp. 375–398, 1994.

[14] M. L. Visinsky, J. R. Cavallaro, and I. D. Walker, "A dynamic fault tolerance framework for remote robots," *IEEE Transactions on Robotics and Automation*, vol. 11, no. 4, pp. 477–490, 1995.

[15] T. C. Lueth and T. Laengle, "Fault-tolerance and error recovery in an autonomous robot with distributed controlled components," in *Proc. of the IEEE International Conference on Robotics and Automation*, pp. 8–13, Springer-Verlag, 1994.

[16] L. E. Parker, "ALLIANCE: An architecture for fault tolerant multirobot cooperation," *IEEE Transactions on Robotics and Automation*, vol. 14, no. 2, pp. 220–240, 1998.

[17] Y. Diao and K. M. Passino, "Intelligent fault-tolerant control using adaptive and learning methods," *Control Engineering Practice*, vol. 10, pp. 801–817, 2002.

[18] Y. Zhang and J. Jiang, "Fault tolerant control system design with explicit consideration of performance degradation," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 39, pp. 838–848, July 2003.

[19] P. Kim, B. C. Williams, and M. Abramson, "Executing reactive model-based programs through graph-based temporal planning," in *Proc. of the International Joint Conference on Artificial Intelligence*, 2001.

[20] B. C. Williams, M. D. Ingham, S. Chung, P. Elliott, M. Hofbaur, and G. T. Sullivan, "Model-based programming of fault-aware systems," *AI Magazine*, vol. 24, no. 4, pp. 61–75, 2003.

[21] B. C. Williams, P. Kim, M. Hofbaur, J. How, J. Kennell, J. Loy, R. Ragno, J. Stedl, and A. Walcott, "Model-based reactive programming of cooperative vehicles for Mars exploration," in *Proc. of the International Symposium on Artificial Intelligence, Robotics and Automation in Space*, 2001.

[22] M. D. Ingham and B. C. Williams, "Timed model-based programming: Executable specifications for robust critical sequences," in *Proc. of the International Workshop on Self-Adaptive Software*, 2003.

[23] M. J. Mataric, "Integration of representation into goal-driven behavior-based robots," *IEEE Transactions on Robotics and Automation*, vol. 8, no. 3, pp. 304–312, 1992.

[24] R. A. Brooks, "A robust layered control system for a mobile robot," *IEEE Journal of Robotics and Automation*, vol. RA-2, no. 1, pp. 14–23, 1986.

[25] D. Dvorak, R. Rasmussen, G. Reeves, and A. Sacks, "Software architecture themes in JPLs Mission Data System," in *Proc. of the IEEE Aerospace Conference*, 2000.

[26] M. Ingham, R. Rasmussen, M. Bennett, and A. Moncada, "Engineering complex embedded systems with State Analysis and the Mission Data System," *AIAA Journal of Aerospace Computing, Information and Communication*, vol. 2, pp. 507–536, December 2005.

[27] R. D. Rasmussen, "Goal-based fault tolerance for space systems using the Mission Data System," in *Proc. of the IEEE Aerospace Conference*, vol. 5, pp. 2401–2410, March 2001.

[28] K. M. Chandy and J. Misra, "Distributed simulation: A case study in design and verification of distributed programs," *IEEE Transactions on Software Engineering*, vol. SE-5, no. 5, pp. 440–452, 1979.

[29] E. Klavins, "A formal model of a multi-robot control and communication task," in *Proc. of the 42th IEEE Conference on Decision and Control*, 2003.

[30] A. E. Haxthausen and J. Peleska, "Formal development and verification of a distributed railway control system," *IEEE Transactions on Software Engineering*, vol. 26, no. 8, pp. 687–701, 2000.

[31] S. Owre, J. Rushby, N. Shankar, and F. von Henke, "Formal verification for fault-tolerant architectures: Prolegomena to the design of PVS," *IEEE Transactions on Software Engineering*, vol. 21, no. 2, pp. 107–126, 1995.

[32] T. Ball and S. K. Rajamani, *SPIN*, vol. LNCS 1885, ch. Bebop: A Symbolic Model Checker for Boolean Programs, pp. 113–130. Springer-Verlag, 2000.

[33] A. Cimatti, E. Clarke, E. Giunchiglia, F. Giunchiglia, M. Pistore, M. Roveri, R. Sebastiani, and A. Tacchella, *CAV*, vol. LNCS 2404, ch. NuSMV 2: An Open Source Tool for Symbolic Model Checking, pp. 359–364. Springer-Verlag, 2002.

[34] J. Burch, E. Clarke, K. McMillan, D. Dill, and L. Hwang, "Symbolic model checking: 10^{20} states and beyond," in *Proc. of the Fifth Annual IEEE Symposium on Logic in Computer Science*, pp. 428–439, 1990.

[35] F. Schneider, S. Easterbrook, J. Callahan, and G. Holzmann, "Validating requirements for fault tolerant systems using model checking," in *Proc. of the Third International Conference on Requirements Engineering*, pp. 4–13, 1998.

[36] A. Biere, A. Cimatti, E. Clarke, and Y. Zhu, *TACAS/ETAPS*, vol. LNCS 1579, ch. Symbolic Model Checking without BDDs, pp. 193–207. Springer-Verlag, 1999.

[37] K. L. McMillan, *CAV*, vol. LNCS 2404, ch. Applying SAT Methods in Unbounded Symbolic Model Checking, pp. 250–264. Springer-Verlag, 2002.

[38] R. Alur, T. Henzinger, and P.-H. Ho, "Automatic symbolic verification of embedded systems," *IEEE Transactions on Software Engineering*, vol. 22, no. 3, pp. 181–201, 1996.

[39] T. A. Henzinger, P.-H. Ho, and H. Wong-Toi, "HyTech: A model checker for hybrid systems," *International Journal on Software Tools for Technology Transfer*, 1997.

[40] K. Larsen, P. Pettersson, and W. Yi, "UPPAAL in a nutshell," *International Journal on Software Tools for Technology Transfer*, vol. 1, no. 1-2, pp. 134–152, 1997.

[41] D. Dill and H. Wong-Toi, *CAV 95: Computer-aided Verification*, ch. Verification of real-time systems by successive over and under approximation, pp. 409–422. Springer, 1995.

[42] G. Frehse, "PHAVer: Algorithmic verification of hybrid systems past HyTech," in *Proc. of the International Conference on Hybrid Systems: Computation and Control*, 2005.

[43] G. Holzmann, *The Spin Model Checker: Primer and Reference Manual*. Addison-Wesley, 2004.

[44] C. Flanagan and P. Godefroid, "Dynamic partial-order reduction for model checking software," *SIGPLAN Not.*, vol. 40, no. 1, pp. 110–121, 2005.

[45] R. Bordini, M. Fisher, W. Visser, and M. Wooldridge, "State-space reduction techniques in agent verification," in *Proc. of the Third International Joint Conference on Autonomous Agents and Multiagent Systems*, pp. 896–903, 2004.

[46] E. Haghverdi, P. Tabuada, and G. J. Pappas, "Bisimulation relations for dynamical, control, and hybrid systems," *Theoretical Computer Science*, vol. 342, no. 2-3, pp. 229 – 261, 2005.

[47] P. Tabuada and G. J. Pappas, "Bisimilar control affine systems," *Systems and Control Letters*, vol. 52, no. 1, pp. 49 – 58, 2004.

[48] A. Girard and G. J. Pappas, "Approximate bisimulation relations for constrained linear systems," *Automatica*, vol. 43, no. 8, pp. 1307 – 1317, 2007.

[49] R. H. Bordini, M. Fisher, W. Visser, and M. Wooldridge, *Programming Multi-Agent Systems*, vol. LNAI 3067, ch. Verifiable Multi-agent Programs, pp. 72–89. 2004.

[50] T. Suzuki, S. M. Shatz, and T. Murata, "A protocol modeling and verification approach based on a specification language and petri nets," *IEEE Transactions on Software Engineering*, vol. 16, no. 5, pp. 523–536, 1990.

[51] R. Simmons, C. Pecheur, and G. Srinivasan, "Towards automatic verification of autonomous systems," in *Proc. of the IEEE/RSJ International Conference on Intelligent Robots and Systems*, vol. 2, pp. 1410–1415, 2000.

[52] A. Holt, "Formal verification with natural language specifications: guidelines, experiments and lessons so far," *South African Computer Journal*, no. 24, pp. 253–257, 1999.

[53] C. A. Vissers, G. Scollo, M. van Sinderen, and E. Brinksma, "Specification styles in distributed systems design and verification," *Theoretical Computer Science*, vol. 89, pp. 179–206, 1991.

[54] R. S. Beata Sarna-Starosta and L. K. Dillon, "A model-based design-for-verification approach to checking for deadlock in multi-threaded applications," in *Proc. of 18th International Conference on Software Engineering and Knowledge Engineering*, 2006.

[55] A. Betin-Can, T. Bultan, M. Lindvall, B. Lux, and S. Topp, "Application of design for verification with concurrency controllers to air traffic control software," in *Proc. of the 20th IEEE/ACM International Conference on Automated Software Engineering*, pp. 14–23, ACM, 2005.

[56] N. Sharygina, J. C. Browne, and R. P. Kurshan, "A formal object-oriented analysis for software reliability: Design for verification," in *Proc. of the Fundamental Approaches to Software Engineering Conference*, pp. 318–332, 2001.

[57] D. Giannakopoulou, C. S. Pasareanu, and J. M. Cobleigh, "Assume-guarantee verification of source code with design-level assumptions," in *Proc. of the 26th International Conference on Software Engineering*, pp. 211–220, IEEE Computer Society, 2004.

[58] T. Bultan and A. Betin-Can, *Verified Software: Theories, Tools, Experiments*, vol. LNCS 4171, ch. Scalable Software Model Checking Using Design for Verification, pp. 337–346. Springer-Verlag, 2008.

[59] G. De Giacomo and M. Y. Vardi, *ECP-99*, vol. LNAI 1809, ch. Automata-Theoretic Approach to Planning for Temporally Extended Goals, pp. 226–238. 2000.

[60] H. Kress-Gazit, G. E. Fainekos, and G. J. Pappas, "Wheres Waldo? Sensor-based temporal logic motion planning," in *Proc. of the IEEE International Conference on Robotics and Automation*, pp. 3116–3121, 2007.

[61] H. Hansson and B. Jonsson, "A logic for reasoning about time and reliability," *Formal Aspects of Computing*, vol. 6, no. 5, pp. 512–535, 1994.

[62] V. Gupta, R. Jagadeesan, and P. Panangaden, "Stochastic processes as concurrent constraint programs," in *Proc. of the 26th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pp. 189–202, ACM, 1999.

[63] H. L. S. Younes, *CAV*, vol. LNCS 3576, ch. Probabilistic Verification for "Black-Box" Systems, pp. 253–265. Springer-Verlag, 2005.

[64] M. Kwiatkowska, "Model checking for probability and time: from theory to practice," in *Proc. of the 18th Annual IEEE Symposium on Logic in Computer Science*, pp. 351–360, June 2003.

[65] A. Aziz, K. Sanwal, V. Singhal, and R. Brayton, "Model-checking continuous-time markov chains," *ACM Transactions on Computational Logic*, vol. 1, no. 1, pp. 162–170, 2000.

[66] J. Sproston, "Decidable model checking of probabilistic hybrid automata," in *Proc. of the 6th International Symposium on Formal Techniques in Real-Time and Fault-Tolerant Systems*, pp. 31–45, Springer-Verlag, 2000.

[67] S. Prajna, A. Jadbabaie, and G. J. Pappas, "Stochastic safety verification using barrier certificates," in *Proc. of the IEEE Conference on Decision and Control*, 2004.

[68] M. Kwiatkowska, G. Norman, and D. Parker, "Probabilistic symbolic model checking with PRISM: a hybrid approach," *International Journal on Software Tools Technology Transfer*, vol. 6, pp. 128–142, 2004.

[69] X. Koutsoukos and D. Riley, "Computational methods for verification of stochastic hybrid systems," *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, vol. 38, pp. 385–396, March 2008.

[70] S. Amin, A. Abate, M. Prandini, J. Lygeros, and S. Sastry, "Reachability analysis for controlled discrete time stochastic systems," in *Proc. of the International Conference on Hybrid Systems: Computation and Control*, pp. 49–63, 2006.

[71] A. Abate, M. Prandini, J. Lygeros, and S. Sastry, "Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems," *Automatica*, vol. 44, no. 11, pp. 2724 – 2734, 2008.

[72] H. A. P. Blom, G. Bakker, and J. Krystul, "Probabilistic reachability analysis for large scale stochastic hybrid systems," in *Proc. of the 46th IEEE Conference on Decision and Control*, pp. 3182–3189, 2007.

[73] S. K. Au and J. L. Beck, "Estimation of small failure probabilities in high dimensions by subset simulation," *Journal of Probabilistic Engineering Mechanics*, vol. 16, 2001.

[74] S. P. Brooks, "Markov Chain Monte Carlo method and its applications," *The Statistician*, vol. 47, no. 1, pp. 69–100, 1998.

[75] C. J. Geyer, "Practical Markov Chain Monte Carlo," *Statistical Science*, vol. 7, no. 4, pp. 473–483, 1992.

[76] D. Dvorak, R. Rasmussen, and T. Starbird, "State knowledge representation in the Mission Data System," in *Proc. of the IEEE Aerospace Conference*, 2002.

[77] D. Dvorak, M. Indictor, M. Ingham, R. Rasmussen, and M. Stringfellow, "A unifying framework for systems modeling, control systems design, and system operation," in *Proc. of the IEEE Conference on Systems, Man, and Cybernetics*, October 2005.

[78] D. Dvorak, "Challenging encapsulation in the design of high-risk control systems," in *Proc. of the ACM Conference on Object Oriented Programming, Systems, Languages, and Applications*, 2002.

[79] G. Labinaz, M. M. Bayoumi, and K. Rudie, "A survey of modeling and control of hybrid systems," *Annual Reviews of Control*, vol. 21, pp. 79–92, 1997.

[80] G. Pola, M. L. Bujorianu, J. Lygeros, and M. D. D. Benedetto, "Stochastic hybrid systems: An overview," in *Proc. of the IFAC Conference on Analysis and Design of Hybrid Systems*, 2003.

[81] J. Hu, J. Lygeros, and S. Sastry, "Towards a theory of stochastic hybrid systems," in *Proc. of the Hybrid Systems: Computation and Control* (N. Lynch and B. Krogh, eds.), vol. Lecture Notes in Computer Science 1809, pp. 160–173, Springer, 2000.

[82] A. Elfes, J. F. Montgomery, J. L. Hall, S. S. Joshi, J. Payne, and C. F. Bergh, "Autonomous flight control for a Titan exploration aerobot," in *Proc of Robotics Science and Systems*, 2005.