Software Fault Tolerance

Projects and Case Studies

Jörg Kienzle
Software Engineering Laboratory
School of Computer Science
McGill University

Programming Project Ideas

- Distributed, Pre-emptive N-Version Programming
- Transactions
  - Nested Transactions
  - Split Transactions
  - SAGAS
  - Open Multithreaded Transactions
- Recovery Blocks
- Consensus Recovery Blocks
- Atomic Actions
- Self-Configuring Optimal Programming
- OPTIMA or AspectOPTIMA
  - Implement parts of OPTIMA in Java
  - Extend AspectOPTIMA with additional features

Airbus

- Pascal Traverse, Dependability of Digital Computers on Board Airplanes, Dependable Computing for Critical Applications, Volume 4, A. Avizienis, J.C. Laprie, editors, 1991, pp. 134 – 152.
- Dominique Briere and Pascal Traverse, AIRBUS A320/A330/A340 Electrical Flight Controls: A Family of Fault-Tolerant Systems, Digest of Papers FTCS-23: The Twenty-Third International Symposium on Fault-Tolerant Computing, June 1993, pp. 616 - 623.
- Torres-Pomales, W., Software Fault Tolerance: A Tutorial, NASA/TM-2000-210616, Langley Research Center, Oct. 2000.
- Naidu, Amit K., Case Study: Airbus A340 Flight Control System, CS651 Dependable Computing, Department of Computer Science, University of Virginia, Dec 2002.
- Airbus Accidents Information
  - http://www.airdisaster.com/
  - http://www.rvs.uni-bielefeld.de/publications/Incidents/

Railway Control

- G. Hagelin, “ERICSSON Safety Systems for Railway Control”, in Software diversity in computerized control systems (U. Voges, Ed.), 2, pp.11-21, Springer-Verlag, 1988.
- G. Mongardi, “Dependable Computing for Railway Control Systems”, in 3rd IFIP Int. Working Conference on Dependable Computing for Critical Applications (DCCA-3), Mondello, Italy, pp. 255-277, 1993.
- H. Kantz and C. Koza, “The ELEKTRA Railway Signalling-System: Field Experience with an Actively Replicated System with Diversity”, in 25th IEEE Annual International Symposium on Fault - Tolerant Computing (FTCS-25), Pasadena, California, pp.453-458, IEEE Computer Society Press, 1995.
- J. F. Lindeberg, “The Swedish State Railways' Experience with n-version Programmed Systems”, in Directions in Safety-Critical Systems (F. Redmill and T. Anderson, Eds.), p.36, Springer-Verlag, 1993.
- D. B. Turner, R. D. Burns and H. Hecht, “Designing micro-based systems for fail-safe travel”, IEEE Spectrum, 24 (2), pp.58-63, 1987.

Others

- CA Actions and the Production Cell
  - A. Zorzo, A. Romanovsky, J. Xu, B. Randell, R. Stroud, I. Welch: "Using Coordinated Atomic Actions to design Complex Safety-Critical Systems: The Production Cell Case Study", Technical Report, University of Newcastle upon Tyne.
  - Many follow-up papers, one in Software Practice and Experience
- Implementations
  - Jie Xu, Brian Randell and Avelino Zorzo: Implementing Software-Fault Tolerance in C++ and Open C++: An Object-Oriented and Reflective Approach.
  - Arjuna & Java OTS
    Shrivastava, S. K.: "Lessons Learned from Building and Using the Arjuna Distributed Programming System", in Theory and Practice in Distributed Systems, pp. 17 – 32, Lecture Notes in Computer Science 938, 1995.