P.O.Box 8718, Beijing 100080, China	Journal of Software Jan. 2003,14(1):54-61
E-mail: jos@iscas.ac.cn	ISSN 1000-9825, CODEN RUXUEW, CN 11-2560/TP
http://www.jos.org.cn	Copyright © 2003 by The Editorial Department of Journal of Software

三机冗余容错系统的描述和验证

郭 亮, 唐稚松

郭 亮, 唐稚松 (中国科学院 软件研究所 计算机科学重点实验室,北京 100080)
第一作者: 郭亮(1976－),男,江西吉安人,博士,主要研究领域为软件工程.
联系人: 郭亮 Telephone: 86-10-62562796, Fax: 86-10-62562533, E-mail: gls@ios.ac.cn
Received 2001-07-30; Accepted 2002-04-10

Abstract
XYZ/E is used to specify and verify the triple-modular redundancy fault-tolerant system. Assuming that each computer is loaded with a determined sequential program P which continuously outputs data to the outer environment, the case P running on single processor is illustrated by an XYZ/E program SingleProcessP, and the property of program P is specified by a temporal logical formula SpecP. Finally, it is proved that the program TripleProcessorsP obtained from the triple-modular redundancy way can still satisfy SpecP in spite of hardware errors.

Guo L, Tang ZS. Specification and verification of the triple-modular redundancy fault-tolerant system. *Journal of Software*, 2003,14(1):54~61.
http://www.jos.org.cn/1000-9825/14/54.htm

摘要
使用XYZ/E描述和验证三机冗余容错系统.考虑每台计算机加载了一个不断向外界环境输出数据的确定性顺序程序P,用XYZ/E程序SingleProcessorP刻画程序P在单机上运行,用时序逻辑式SpecP刻画P向外部环境输出的数据所满足的性质.最后证明,采用三机冗余模式所得到的程序TripleProcessorsP即使在出现硬件错误的情况下运行,也能满足性质SpecP.

基金项目：Supported by the National Natural Science Foundation of China under Grant No.60073020 (国家自然科学基金); the National High Technology Development 863 Program of China under Grant No.863-306-ZT02-04-01 (国家863高科技发展计划)

References:

[1] Schepers H. Terminology and paradigms for fault tolerance. In: Vytopil J, ed. Formal Techniques in Real-Time and Fault Tolerant Systems. Boston: Kluwer Academic Publishers, 1993. 3~31.

[2] Doug GW. Fault tolerance as self-similarity. In: Vytopil J, ed. Formal Techniques in Real-Time and Fault Tolerant Systems. Boston: Kluwer Academic Publishers, 1993. 33~49.

[3] Liu ZM, Joseph M. Specification and verification of fault-tolerance, timing and scheduling. ACM Transaction on Programming Languages and Systems, 1998,21(1):46~89.

[4] Liu ZM, Joseph M. Transformation of programs for fault-tolerance. Formal Aspects of Computing, 1992,4(5):442~469.

[5] Liu ZM. Fault-Tolerant programming by transformations [Ph.D. Thesis]. Department of Computer Science, University of Warwick, 1991.

[6] Lamport L. The temporal logic of actions. ACM Transactions on Programming Languages and Systems, 1994,16(3):872~923.

[7] Abadi M, Lamport L. The existence of refinement mapping. Theoretical Computer Science, 1991,83(2):253~284.

[8] Tang ZS. An introduction to XYZ system. Technical Report, ISCAS-XYZ-88-1, Beijing: Institute of Software, the Chinese Academy of Sciences, 1988.

[9] Tang ZS. Temporal Logical Programming and Software Engineering. Beijing: Science Press, 1999 (in Chinese).

附中文参考文献:
[9] 唐稚松.时序逻辑程序设计与软件工程.北京:科学出版社,1999.