P.O.Box 8718, Beijing 100080, China	Journal of Software, June 2004,15(6):823-833
E-mail: jos@iscas.ac.cn	ISSN 1000-9825, CODEN RUXUEW, CN 11-2560/TP
http://www.jos.org.cn	Copyright © 2004 by The Editorial Department of Journal of Software

基于体系结构模型检查分布式控制系统

汪 洋, 魏 峻, 王振宇

汪 洋1,2,3, 魏 峻1,3, 王振宇2,3, 1(中国科学院 软件研究所,北京 100080)2(武汉数字工程研究所,湖北 武汉 430074)3(武汉大学 软件工程国家重点实验室,湖北 武汉 430072)
作者简介: 汪洋(1968－),男,湖北麻城人,博士生,主要研究领域为软件工程,分布式系统,中间件技术;魏峻(1970－),男,博士,副研究员,主要研究领域为软件工程,软件理论,网络分布式计算技术;王振宇(1936－)男,研究员,博士生导师,主要研究领域为软件工程,软件理论与工具开发.
联系人: 汪 洋 Phn: +86-10-62630989, E-mail: yangwang@public.wh.hb.cn, http://www.iscas.ac.cn
Received 2003-08-13; Accepted 2003-11-27

Abstract
Distributed control systems are a category of high complex systems that include a large number of devices controlled and harmonized by computer systems. Their reliability and functional correctness always need to be guaranteed as their mission-critical feature. The analysis process for complex control systems consists of proving or verifying that the designed system indeed meets certain specifications. However, both the design and analysis may be formidable due to the complexity and magnitude of the system. From an analysis perspective, the complexity of a system can be reduced by imposing a hierarchical structure and abstraction on the architectural design. Currently, model checking has been demonstrated by more and more successes. It is an effective way to verify that the construction of a complex system satisfies to the requirements of reliability and correctness. In this paper, an approach for formally analyzing distributed control systems at architectural level by applying software architecture description and model checking techniques is presented. Through study on a building comprehensive control system, it is shown that the method could improve the quality of design of distributed control systems.

Wang Y, Wei J, Wang ZY. Model checking distributed control systems based on software architecture. *Journal of Software*, 2004,15(6):823~833.
http://www.jos.org.cn/1000-9825/15/823.htm

摘要
分布控制系统是大量硬件设备通过计算机系统得以控制和协调的高度复杂系统,它们也是任务关键的系统,需要保障其功能的高度正确性和可靠性.分析复杂控制系统的过程包含了证明或验证设计的系统确实满足某种需求.但由于系统的复杂度,有效分析系统是相当困难的.从系统设计和分析的角度看,基于体系结构方法可以运用层次化构造和抽象的方法来减小模型复杂度.模型检查技术是分析复杂系统构造满足正确和可靠性需求的有效方法.结合软件体系结构描述方法和模型检查技术,提出了基于体系结构的分布式控制系统形式分析方法,通过楼宇综合控制系统实例研究,展示了该方法在提高分布式控制系统设计质量方面的效果.

基金项目: Supported by the National Natural Science Foundation of China under Grant No.60203029 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant No.2001AA113010 (国家高技术研究发展计划(863)); the National Grand Fundamental Research 973 Program of China under Grant No.2002CB312005 (国家重点基础研究发展规划(973))

References:

[1] Pappas GJ, Sastry S. Towards continuous abstractions of dynamical and control systems. In: Antsaklis P, Kohn W, Nerode A, Sastry S, eds. Hybrid Systems IV. Lecture Notes in Computer Science 1273, New York: Springer-Verlag, 1997. 329~341.

[2] Clarke E, Grumberg O, Peled D. Model-Checking. MIT Press, 1999.

[3] Holzmann GJ. The spin model checker. IEEE Trans. on Software Engineering, 1997,23(5):279~295.

[4] McMillan K. Symbolic Model Checking. Boston: Kluwer Academic Publishers, 1993.

[5] Magee J, Kramer J. Concurrency: State Models & Java Programs. Indianapolis: John Wiley & Sons, 1999.

[6] Holzmann GJ. Design and Validation of Computer Protocols. Englewood Cliffs: Prentice-Hall, 1991.

[7] Manna Z, Pnueli A. The Temporal Logic of Reactive and Concurrent Systems: Specification. New York: Springer-Verlag, 1991.

[8] Hoare CAR. Communicating Sequential Processes. Englewood Cliffs: Prentice-Hall, 1985.

[9] Allen R, Garlan D. A formal basis for architectural connection. ACM Trans. on Software Engineering and Methodology, 1997, 6 (3):213~249.

[10] Inverardi P, Wolf AL. Formal specifications and analysis of software architectures using the chemical abstract machine model. IEEE Trans. on Software Engineering, 1995,21(4):100~114.

[11] Magee J, Kramer J, Giannakopoulou D. Behaviour analysis of software architectures. In: Donohoe P, ed. Proc. of 1st Working IFIP Conf. on Software Architecture (WICSA1). Boston: Kluwer Academic Publishers, 1999. 35~50

[12] Garlan D, Khersonsky S, Kim JS. Model checking publish-subscribe systems. In: Ball T, Rajamani SK, eds. Proc. of the 10th SPIN Workshop: Model Checking Software. Heidelberg: Springer-Verlag, 2003. 166~180.

[13] Inverardi P, Muccini H, Pelliccione P. Automated check of architectural models consistency using SPIN. In: Feather M, Goedicke M, eds. Proc. of the 16th IEEE Int'l Conf. on Automated Software Engineering (ASE 2001). Los Alamitos: IEEE Computer Society Press, 2001. 346~349.

[14] Issarny V, Kloukinas C, Zarras A. Systematic aid in the development of middleware architectures. Communications of the ACM, 2002, 45 (6):53~58.

[15] Bachmann F, Bass L, Chastek G, Donohoe P, Peruzzi F. The architecture based design method. Technical Report, CMU/ SEI-2000-TR-001, Pittsburgh: Software Engineering Institute, Carnegie Mellon University, 2000.

[16] Eugster P, Felber PA, Guerraoui R, Kermarrec AM. The many faces of publish/subscribe. ACM Computing Surveys, 2003,35(2): 114~131.

[17] Taylor RN, Medvidovic N, Anderson KM, Whitehead Jr. EJ, Robbins JE, Nies KA, Oreizy P, Dubrow DL. A component- and message-based architectural style for GUI software. IEEE Trans. on Software Engineering, 1996,22(6):390~406.

[18] Dwyer MB, Avrunin GS, Corbett JC. Patterns in property specifications for finite-state verification. In: Proc. of the 21st Int'l Conf. on Software Engineering. Los Alamitos: IEEE Computer Society Press, 1999. 411~420.

[19] Comella-Dorda S, Gluch D, Hudak J, Lewis G, Weinstock C. Model-Based verification: Claim creation guidelines. Technical Note, CMU/SEI-2001-TN018, Pittsburgh: Software Engineering Institute, Carnegie Mellon University, 2001.

[20] Wang Y, Wang ZY. Design and implementation of intelligent building management system based on CORBA. Computer and Digital Engineering, 2001,29(2):16~22 (in Chinese with English abstract).

附中文参考文献:

[20] 汪洋,王振宇.基于CORBA的智能建筑管理系统IBMS的设计与实现.计算机与数字工程,2001,29(2):16~22.