Formal Modeling and Correctness Proof of Spatial Partition Algorithm

Liping Zhu, Fangfang Wu, Pei Yang, Jixun Yan, and Li Ma

Abstract In the development of the embedded real-time operating system which follows ARINC653 (Standard Interface of Avionics Application Software), the partition protection and address translation algorithm of the memory management unit based on PowerPC E200 processor is proposed and formally verified. Using the interactive theorem proving tool Coq, firstly, address translation is formally modeled. Secondly, the three requirements that the algorithm must meet are expressed in the form of theorems. Finally, the strategies and construction methods of the tool are used to prove the correctness of the algorithm. The algorithm verification results show that the formal method theoretically guarantees the correctness of the key algorithm of the operating system, overcomes the incompleteness of the traditional test methods, and provides a strong guarantee for the development of high-quality safety critical software.

L. Zhu (✉) · F. Wu · P. Yang · J. Yan · L. Ma
AVIC Xi'an Flight Automatic Control Research Institute, Jinye Road 129, Xi'an, China
e-mail: zlponline@163.com

D. Krob et al. (eds.), *Complex Systems Design & Management*,
https://doi.org/10.1007/978-3-030-73539-5_43