Failure Boundedness in Discrete Applications

João Muranho[1], Paula Prata[1], Mário Zenha-Rela[2], João Gabriel Silva[2]

[1] Department of Informatics, Universidade da Beira Interior,
P 6201-001 Covilhã, Portugal
[2] University of Coimbra (UC),
CISUC, Department of Informatics Engineering, P 3030-290 Coimbra, Portugal
{muranho, pprata}@di.ubi.pt, {mzrela, jgabriel}@dei.uc.pt

Abstract. Computer control of discrete applications present a challenging dependability problem since any wrong output may lead the system to a completely anomalous state. This is in contrast with continuous feedback systems where wrong outputs can only gradually deviate the system under control from its intended set point. Transient errors may even be filtered by the latency inherent to the physical application. In this paper we extend our previous experimental research on the use of the fail-bounded model in continuous feedback systems into discrete control applications in order to evaluate whether it could be applied to this kind of problems. The reset-driven approach was used as the basic error detection and recovery mechanism complemented by assertions based on the Petri Net modeling of the problem, thus taking advantage of the discrete nature of the applications. The well-known semaphore control problem is used as testbed for experimental evaluation by fault-injection in the controller. The main contribution of this paper is to present experimental data showing that effectively the fail-bounded model can be applied to discrete applications whenever a continuous physical system exists in the control loop.

Keywords: Failure avoidance, Discrete applications, Fail-bounded model, Petri nets, Experimental Dependability Evaluation.

Acknowledgments

This work was partially supported by the Group of Networks and Multimedia of the Institute of Telecommunications (IT) Covilhã Lab, Portugal; and by Portuguese Ministry of Education through program Prodep III-Action 5.3-project 185.009.