UNIVERSITÄT HEIDELBERG

International Workshop on the
Design of Dependable Critical Systems

ECOMODIS

Proceedings

of the
International Workshop on the
Design of Dependable Critical Systems
"Hardware, Software, and Human Factors in Dependable System Design"

DDCS 2009

September 15, 2009
Hamburg, Germany

In the framework of
The 28th International Conference on
Computer Safety, Reliability and Security
SAFECOMP 2009

Edited by

Achim Wagner[1], Meike Jipp[1], Colin Atkinson[2] and Essameddin Badreddin[1]

[1] Automation Laboratory, Institute of Computer Engineering, University of Heidelberg
[2] Chair of Software Engineering, University of Mannheim

ziti

International Workshop on
the Design of Dependable Critical Systems
September 15, 2009, Hamburg, Germany

Hierarchical Hybrid Monitoring for Autonomous Systems

Leila Zouaghi, Achim Wagner, and Essameddin Badreddin

Automation Laboratory, University of Heidelberg, Germany
{leila.zouaghi, achim.wagner, badreddin}@ziti.uni-heidelberg.de

Safety critical computer systems such as control systems for automobile, aircraft, medical and intelligent mobile robots, are rapidly growing in complexity. This increasing complexity has made system monitoring an inevitable component of system operations and the subject of intensive study in the past few years. Several methods are used to deal with hybrid systems monitoring, which are based on multi-model numerical filters, such as the Kalman filter [1] or particle filtering methods [2], [3]. Other approaches are based on automata [4] or on Bayesian nets [5] linked to some numerical evolution models. The only existing monitoring approach based on Particle Petri net was used for the analysis of flight procedures and deals with situation monitoring [6]. We consider a general, nonlinear, distributed, complex system with hybrid (discrete/continuous) behavior, for which a monitor has to be designed. Such systems present significant challenges for monitoring and diagnosis. For a large number of states and highly nonlinear equations, the design of a monitor is clearly problematic.

Our approach gives a solution to reduce the design complexity by decomposing such a system using separate monitors for each subsystem. In this context, we have proposed a model of hierarchical hybrid monitoring for systems with so called "Recursive Nested Behavior Control" (RNBC) structure, which has been successfully employed for autonomous mobile robots [7], [8]. Since the system architecture is nested, the monitoring system is built using a nested structure. In this scheme, the monitors of a subsystem work independently using recursively the results of the monitors of the lover levels. The monitoring concept of the RNBC is shown in Fig.1.

The hybrid state estimation is performed using a particle Petri net [9] model. It allows the representation of the discrete dynamics of the system through the Petri net structure and the modeling of the continuous behavior by evolution equations. The estimator is based on the particle filtering principle and computes the expected markings of the particle Petri net. From the estimation of the marking of the Petri net inconsistent behaviors can be detected. The consistency is checked with respect to the reachable markings of the Petri net.

This work addresses the challenge of the interaction between continuous and discrete dynamics for the monitoring of autonomous systems with nested structure. The novelty of the framework is the use of the Particle Petri net for the monitoring of systems with a Recursive Nested control structure and the methodology for detecting

discrepancies between the expected and the actual behaviour of the system in such structure. The nested hybrid estimation methodology has been demonstrated on a heating control system example. The simulation results show the feasibility of the proposed design.

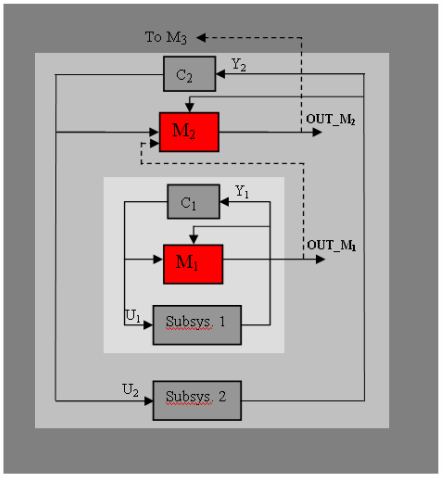

Figure 1. Monitoring structure.

References

1. Veeraraghavan, H. and Papanikolopoulos, N.: "Combining multiple tracking modalities for vehicle tracking in traffic intersections". In IEEE International Conference on Robotics and Automation (ICRA), USA, 2004.
2. Koutsoukis, X., Kurien, J. and Zhao, F.: "Monitoring and Diagnosis of hybrid systems using particle filtering methods". Proc. Mathematical Theory of Networks and Systems (MTNS), 2002.
3. Verma, V.: Tractable Particle Filters for Robot Fault Diagnosis. Doctoral dissertation, Robotics Institute, Carnegie Mellon University, May, 2005.
4. Hofbaur, M. and Williams, B. : "Mode estimation of probabilistic hybrid systems". In International Workshop on Hybrid Systems, Computation and Control (HSCC), Stanford, California, USA, 2002.
5. Lerner, U., Moses, B., Scott, M., McIlraith, S., Koller, D.: Monitoring a complex physical system using a hybrid dynamic Bayes net. In: UAI'02, Edmonton, AB (2002)
6. Lesire, C., Tessier, C.: Particle Petri nets for aircraft procedure monitoring under uncertainty. In: ATPN'05, 26 th International Conference On Application and Theory of Petri Nets and Other Models of Concurrency, Miami, FL (2005)
7. Badreddin, E. "Recursive Control Structure for Mobile Robots", International Conf. on Intelligent Autonomous Systems 2 (IAS.2), Amsterdam, pp. 11-14, 1989.
8. Badreddin, E., "Recursive Behaviour-based Architecture for Mobile Robots", Robotics and Autonomous Systems, VO1.8, 1991
9. Lesire, C. et Tessier, C. : Réseaux de petri particulaires pour l'estimation symbolico-numérique. In Journées Formalisation des Activités Concurrentes (FAC), Toulouse, France, 2005b.