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

# Dependable component-based design on the Example of a Heating Control System

Leila Zouaghi[1], Markus Koslowski[1], Alexander Alexopoulos[1], Florian Barth[2], Meike Jipp[1], Raul Fajardo[3], Yi Luo[1], Achim Wagner[1], Essameddin Badreddin[1]

[1]Automation Laboratory, University of Heidelberg, Germany
{leila.zouaghi, markus.koslowski, alexander.alexopoulos, meike.jipp, yi.luo, achim.wagner, badreddin}@ziti.uni-heidelberg.de
[2] Chair of Software Engineering, University of Mannheim, Germany
barth@informatik.uni-mannheim.de
[3] Department for Application Specific Computing, University of Heidelberg, Germany
raul.fajardo@ziti.uni-heidelberg.de

This poster illustrates new methodologies for the design and the realization of dependable component-based systems covering hardware, software and human factor aspects. The system structure uses the approach of the "Recursive Nested Behavior Control" (RNBC) ensuring dependable operation and seamless interaction of the system's components [1]. For the design and the specification of the system the component based design Method KobrA [2] is applied. The specification of hardware components based on high-level hardware design, Transaction-Level Model [3], is presented. Dependability relevant concepts such as Quality of Service and built-in tests using test- sheets [4] as a new way of defining the expected functionality of a component are introduced. For the on-line monitoring of the system we propose a particle Petri net model. This model allows the estimation of the hybrid state of the system and the detection of discrepancies between the expected nominal behavior of the system and the observed one. For a better reflexion of the reality we model both discrete and continuous state of the behaviour. An integrated dependability model has been developed which includes system, hardware, software, and human properties on a behavioural view. It defines, how much the system's behaviour deviates from the desired behaviour over the system's mission (usage) and how much the system's behaviour keeps away from the non-desired (critical) behaviour. A literature review has shown that quantitative descriptions of system dependability are generally done over combinations of some attributes [5], [6]. These attributes are: reliability, availability, safety, integrity, confidentiality and maintainability. We introduce a behaviour based modelling approach [7], [8], [9]. A dependability metric was developed, which can be used during design respectively during run-time to measure the sub-systems' as well as the overall system's dependability. To be able to measure the involved dependability attributes during run-time built-in test software modules have been generated based on test-sheets.

Approaches for the design of Human-Technology Interaction adapt the technical system to the operator only in a very general way and ignore differences between operators. We adapt the technical system and its interface to the abilities of the operator and take into account the individual differences in these abilities between and within operators [10]. The interfaces are adapted so that its demand character

does not exceed the ability level of the operator. While for some operators it is easier to interpret figural information, figural information will be displayed. Others prefer verbal and numerical information, so that for them, the relevant contents are displayed in the numerical and verbal representation.

In order to demonstrate the feasibility of the proposed methods and techniques (system architecture, dependability modeling and measure, component-based software and hardware design, testing using test sheets, monitoring, human-technology interaction etc.) we use a simple case study from the control engineering domain: Heating Control System (HCS), which is responsible for maintaining a comfortable temperature in a house by regulating the temperature of the available radiators. Using this case study, in which scientist from different disciplines and application domains were involved, the developed methods were tested and adapted. The achieved interesting results show the feasibility of the proposed methods and their usability for the design and the realization of dependable systems.

## References

[1] Badreddin, E. “Recursive Control Structure for Mobile Robots”, International Conf. on Intelligent Autonomous Systems 2 (IAS.2), Amsterdam, pp. 11-14, 1989.

[2] Atkinson C., Bostan P., Brenner D., Falcone G., Gutheil M., Hummel O., Juhasz M. & Stoll D. (2008). Modeling Components and Component-Based Systems in KobrA , to appear in A. Rausch, R. Reussner, R. Mirandola, F. Plasil (eds.): The Common Component Modeling Example: Comparing Software Component Models, Springer

[3] Cai, L., Gajski, D., Transaction level modeling in system level design, Tech. Rep., Center for Embedded Computer Systems, Irvine, Calif, USA, 2003.

[4] Atkinson C. & Brenner D. (2008). Software Testing using Test Sheets, submitted to International Symposium on Software Testing and Analysis (ISSTA), Seattle, Washington, July 20-24 2008

[5]Laprie, J. C. Dependable computing: BASIC concepts and terminology: in english, french, german, italian and japanese. Ed. Springer – Verlag, 1992

[6]Laprie, J.C., (1995). Dependable Computing and Fault Tolerance: Concepts and Terminology. Fault-Tolerant Computing, 1995, ' Highlights from Twenty-Five Years'., Twenty-Fifth International Symposium on, p. 2.

[7]Rüdiger, J., Wagner, A., & Badreddin, E. (2007a). Behavior based definition of dependability for autonomous mobile systems. European Control Conference (July, 2007). Kos, Greece.

[8]Rüdiger, J., Wagner, A., & Badreddin, E. (2008a). Behavior based dependability estimation. ICINCO. Funchal, Madeira - Portugal.

[9]Rüdiger, J., Wagner, A., & Badreddin, E. (2008b). Behavior based estimation of dependability for autonomous mobile systems using particle filter. IFAC. Seoul, Korea.

[10] Jipp, M., Wagner, A., & Badreddin, E. (2008), Individual Ability-Based System Design of Dependable Human-Technology Interaction. International Proceedings of the IFAC World Congress in Seoul, South Corea.