Component Models for Dependable Systems

M.R.V. Chaudron & J. Muskens
Technische Universiteit Eindhoven
PO Box 513, 5600 MB Eindhoven, The Netherlands
{m.r.v.chaudron, j.muskens}@tue.nl

Component-based Software Engineering (CBSE) is a maturing paradigm for conquering the complexity currently faced in software development. In the development of component-models, most attention has been paid to achieving interoperability at a technical level. However, many application domains require that systems meet extra-functional requirements, such as timeliness, safety, low-resource use, reliability.

Systems with dependability properties can only be achieved from building-blocks that are designed to meet dependability properties. The engineering of dependable systems from components can be simplified by defining a suitable component-model. Such a component model defines a set of rules and principles that govern the design of components and connectors as well as the facilities provided by development- and run-time infrastructures. Examples of such facilities are specific approaches for specification, analysis and integration of components.

This session introduces 8 papers in the area of component models for dependable systems. These papers are grouped into 3 themes.

The first theme is the design of component models for domains with specific extra-functional requirement. In this session Hansson et.al. present a component model that is tailored for real-time and safety requirements.

The second theme deals with analysis and validation techniques. In the CBSE paradigm there is an increasing trend towards performing such validation and analyses at run-time. In this session, 3 papers will be presented. The papers in this theme address: the procedures necessary for component certification (Mei et.al.), the validation of real-time properties using a scenario-based approach (Bondarev et.al), and a method for detection heap management flaws in component-based systems (Verta et.al.).

The third theme is about frameworks for component-based systems that enhance dependability. A framework is a set of services/facilities that can be used in combination with a core component model to cater for a specific issue. Sometimes such frameworks can be tailored or extended for a particular application. This theme includes 4 papers.

The first paper (by Telea et.al) describes a framework for the visualization of component systems, and its application on three examples. A possible use of this framework is for the remote monitoring and management of a large population of components that are deployed across a number of devices. The second paper in this theme presents an approach for exception handling in component-based systems. The paper advocates a combination of local (per-component) exception handling and global (inter-component) exception handling strategies. The paper by Ramasamy et.al. proposes a framework for intrusion tolerance. The goal of intrusion tolerance is to ensure that system will remain operational despite malicious faults due to intrusion. Another approach to increasing the dependability is proposed in the paper by Muskens et.al. This paper proposes a formal self-model that can be used by a system itself or by remote parties to monitor a system’s integrity.