Abstract

Advanced embedded systems increasingly contain self-optimizing behavior to improve or maintain properties like quality of service, dependability, or performance in spite of failures or environmental changes. As embedded systems are often employed in a safety-critical context, the effects of self-optimization on the safety must be analyzed carefully. Self-optimization is usually implemented by software and results in the exchange of system components at runtime which means a change of the architecture.

This thesis presents a hazard analysis approach for such systems which is geared especially towards the properties of self-optimizing systems, e.g. architectural reconfiguration for behavioral adaptation.

The hazard analysis is based on a specification of the errors and failures of individual components as well as their propagation in the system's component structure. This specification enables qualitative and quantitative hazard analyses. For the special case of self-optimizing systems, the different configurations of the system's component structure are taken into account.

The hazard analysis approach contains a modeling language for the structure and structural reconfigurations. The specification of structure is based on UML component diagrams and composite structures. The accompanying language for structural reconfigurations combines graph transformations with the concrete syntax of component diagrams for a tight integration with the modeling language for component structures.

Examples from the RailCab-Project are used to illustrate the presented concepts. The hazard analysis has been implemented prototypically in the Fujaba4Eclipse case tool.