TU Dresden

Fakultät Elektrotechnik und Informationstechnik

Institut für Automatisierungstechnik

Thesen zur Dissertation:

Contributions to the Model-based Analysis of Timing Errors for Reliable Design of Mechatronic Systems

Thomas Mutzke

Mechatronic systems are integrated systems that combine mechanical engineering, electronics, computer science, and control engineering to create innovative and automated technologies. Examples of mechatronic systems include e.g. robots, automotive systems, consumer products, and medical devices. Such systems typically comprise distributed components with embedded controllers that run in parallel and share data over a communication network.

1. For proper system behavior, the components need to work flawlessly together. Factors such as concurrency, synchronization, temporal sequence, and timing significantly impact the system's behavior.
2. The detection of design errors during the system test and verification stage typically causes high costs and efforts for a redesign.
3. The model-based systems analysis (MBSA) supports mechatronic system design since it allows the analysis and prediction of system behavior without a physical prototype available. The MBSA requires the generation of abstract models that are used to analyze the behavior. It helps to increase the maturity of the design, to compare design alternatives, and to support design decisions.
4. The benefits of the MBSA are saving time and cost in product development by detecting specification inconsistencies and design errors in early design phases, evaluating various design options, and finding design solutions that fit the specified requirements.
5. The assessment of the system's reliability is challenging, but also beneficial in the MBSA because it helps estimate reliability metrics. One threat to the system's reliability is the faulty interaction of its components. Timing is crucial for this interaction. The occurrence of timing errors can affect the reliability, e.g., if the temporal behavior is not as expected due to varying execution times or communication delays.
6. For widely used modeling languages such as UML and SysML, only semi-formal semantics are specified. This fact is the main motivation for transforming the baseline model, e.g., a SysML activity diagram, into a formal model, e.g., a Petri net model. The state-of-the-art approaches for the model-based timing analysis typically propose a model-to-model transformation, where the generated model

allows the formal analysis of timing properties. In these approaches, the annotation of timing properties is usually limited to specific distributions or intervals, and the inherent timing constraints caused by the interaction of the control and data flow in the baseline model are not considered.

7. Stochastic Petri nets are recognized as useful modeling tools for analyzing the performance and reliability of systems.
8. The main contribution of this thesis is a holistic approach for the model-based analysis of the timing behavior of mechatronic systems in the early stages of the system design that enables the assessment of timing errors. It comprises (i) the specification of appropriate annotation of timing properties in the baseline model based on the assumption that the timing is not deterministic but stochastic, (ii) the definition of a model-to-model transformation from the baseline model into a formal stochastic Petri net model that allows an automated transformation of models, which are specified in a standard XMI format, and (iii) an approach for extracting and formalizing timing constraints.
9. The approach enables specifying stochastic timing properties as general user-defined contributions with few assumptions on the control flow in the baseline model.
10. A sensitivity analysis reveals the contribution of the specific model parameter to the computed results and helps to identify appropriate candidates to improve the design.
11. The introduced method allows for revealing shortcomings in the system design regarding the timing behavior in early design stages. It helps increase the maturity of the design before implementing the real system and may avoid timely and expensive redesign in later design stages.