TU Clausthal

Bachelor-, Master- und Doktorandenseminar
des Instituts für Informatik

Model-based safety analysis of a medical device using SCADE

Sara Mahvi, B.Sc., TU Clausthal

In recent development, many of the complex modern systems, which contribute to safety, are controlled by software. In the medical domain, infusion pumps are one of the safety-critical medical devices which are controlled through their microprocessor. This thesis analyzes the Patient Controlled Analgesia (PCA) pump which is a family of infusion pumps. Recently some problems have been discovered in Generic Infusion Pump (GIP) by US Food and Drug Administration (FDA), which lead to serious problems for patients.

This thesis aims to compare safety analysis techniques and also to indicate to what extent the quality of safety analysis can be improved by using formal modeling. We illustrate this approach with the help of PCA pump.

The model-based safety analysis is an important part of developing a safety critical system. It is a complete and accurate analysis on the components of system and specifies why a component fails and causes a system hazard.

The process begins with conducting four different types of hazard analysis techniques to PCA pump such as: FMEA, FTA, CFT and STPA. Then we compare these techniques with each other and explain the results. After applying hazard analysis techniques to the PCA Pump, we derive system safety requirements to prevent and mitigate identified hazards. In the next step, a PCA model is created in SCADE Suite based on component based requirements that we have derived from safety analysis techniques. SCADE Suite is a tool for developing critical embedded model-based designs. We formalize the PCA components error models and combine them to the existing component models. The error model is a state machine that attach to components of the model in order to identify the faults of system in the presence of failure. Then we can simulate the complete PCA model in SCADE and find the bugs of design. Finally, after simulation and elimination of errors, the model should be verified based on system safety requirements.

The last step is formal verification of the PCA model. We have done the verification phase using Design Verifier, which is an automated analysis tool in SCADE Suite. The importance of the verification phase is that it proves whether the model holds the safety requirements, in presence of faults or not. We have verified the PCA model based on eleven safety requirements.

Montag, den 29.09.2014
14 Uhr s.t. in Raum 210, IfI, Am Regenbogen 15

Technische Universität Clausthal • Institut für Informatik • Julius-Albert-Straße 4 • 38678 Clausthal-Zellerfeld
Tel +49.(0)5323.72.7100 • Fax +49.(0)5323.72.7139 • http://www.in.tu-clausthal.de • info@in.tu-clausthal.de