Interactive Visualization supporting Safety Analysis (Minimal Cut Set Analysis) of Embedded Systems Hardware

Yasmin I. Al-Zokari

Nowadays, embedded systems are commonly used. Embedded System’s complexity can vary from low, e.g., a single micro-controller chip, to very high, e.g., robots. In order to assure the safety of the embedded system to living beings and/or the environment, the systems should be examined and analyzed. It is extremely difficult to analyze safety issues in complex embedded systems using only the standard methods and tools, because of the large amount of data coming from, e.g., fault tree analysis or the model structure. This analysis is done by selecting the most critical group of components to be recovered or improved. It is very difficult and cumbersome to explain and understand a huge amount of complex information quickly and clearly, even when the data represents only the hardware and structure of the system being analyzed. It is even more difficult to relate the results of the safety analysis to the actual parts of the system. Even more, the communication between both safety analysts and mechanical engineers to exchange their knowledge about the system under analysis is very difficult. Until now, there is a lack of sophisticated metaphors that support the efficient visualization of the results of fault tree analysis, such as minimal cut sets and to link the knowledge of the “safety” and the “mechanical engineering” domains [7]. For this work, we took foundations from both domains, linked them, and provided an easy clear and intuitive way for representing them to the analysts and engineers. We provided a visualization system to ease the search and exploration of the critical components given by the safety analysis. Additionally, it eases the understanding of the physical structure of the system under analysis. Finally, it shows the possible faulty system’s components in the model directly [9, 5]. Many quantitative and qualitative evaluations were performed and the results used to improve the usability and the usefulness of the system [6, 8]. The results from the last formal evaluation showed that this system was significantly better than one of the standard tools for safety analysis. The accuracy increased remarkably from above 28.7% for the standard system to above 83.1% for the visualization system, with a no significant difference in the average time performing the tasks. This work in partially funded by DAAD [2], and the BMBF project ViERforES I [3, 4].

Bibliography