

0.1 Visual Support of Safety Analysis Aspects in Embedded Systems

Raghd Tarawneh (tarawneh@cs.uni-kl.de)
Supervisor: Prof. Achim Ebert

Embedded systems² are widely used in most of our daily activities. Generally, embedded systems consists of hardware and software components. Usually, most embedded systems may become very large. Therefore they are not centralized in one component, but they are distributed among a set of components representing the system parts. The system components communicate with each other via a set of hardware/software interfaces. As the size of such a system increases, the task of analysing the failure becomes more difficult. The process of analysing failures to trace the reasons behind them is considered to be a crucial task. Many techniques were proposed to trace the failure propagation paths among the set of the cooperating components in the embedded system. The Fault Tree (FT)¹ technique is a common modelling technique that helps to understand the failure mechanisms of certain systems. FT describes on a logical basis the relationship between component failures and undesired system states/failures. As a descendant of this model, the Component Fault Tree(CFT)¹ concept came to extend the FT concept by introducing additional information about the system structure. Fault trees of complex systems are often very large. The process of analysing and tracing the failure paths in such a large structure becomes a tedious task. In this research we aim to get an overview about the set of components involved in a given failure mechanism. Moreover, we aim to provide a means for the visual comparison of the components with respect to safety criticality. Also, providing insights about the way components might contribute to an undesired system failure. To achieve that, we map the elements of the FT to visual elements in the our final layout. We accomplish that by providing a VR environment allowing to explore certain safety scenario in the 3D model for the hardware components. The 3D model is integrated with an abstract representation of the failure mechanism of the corresponding software components. We use graph visualization³ techniques to show the infected software components of the embedded system. Beside that we visualize the failure path between the different system components. And provide interaction techniques allowing to efficiently cope with the represented data.

¹Kaiser, Bernhard and Liggesmeyer, Peter and Mäckel, Oliver, *A New Component Concept for Fault Trees*

²Edward A. Lee and Sanjit A. Seshia, *Introduction to Embedded Systems - A Cyber-Physical Systems Approach* 2010

³Herman,I. and Melancon, G. and Marshall, M. S. *Graph visualization and navigation in information visualization: A survey*, year = 2000