Embedded System Quality and Safety Analysis

Failure Mode and Effects Analysis

Brigitte Andrich

When safety analysis techniques are applied on a new design, the primary objective is to anticipate potential scenarios of failure in the system under consideration.

The focus of this thesis is the application of Failure Mode and Effects Analysis (FMEA) to software. For that, the SAE J1739 standard for FMEA (for electrical and mechanical hardware) is modified and extended to the analysis of software.

The FMEA is considered for two different areas: The design phase, and the post-coding phase of the product.
Simplifications for the FMEA process, possibilities for automation, and their quality-impact on the FMEA are investigated.
Ideas for improvements and extensions, like an alternative Risk Priority Number calculation are stated.
The FMEA method is compared with similar analysis techniques. Some strengths of other analysis techniques are adapted to the FMEA method.
Benefits of supporting the FMEA process with additional safety analysis methods, like Fault Tree Analysis, Block Diagrams, Cause-Consequences Analysis, are also investigated.
The result is a variety of different possibilities for implementing a FMEA. The outputs vary in quality. Different quality levels for the implementation of a FMEA are established, and graphically portrayed in a pyramid.
The FMEA process is split up into five steps. These steps are further refined through activities. Dependencies among the different activities are portrayed.
A Case Study, in cooperation with MAGNA STEYR Fahrzeugtechnik AG & Co KG (MSF), is performed, in order to gain experience, evaluate the FMEA, and refine the FMEA process.

It is planned to finish the thesis at the end of July, 2004.

Gerald Stieglbauer 2004-03-18