Fehlerbaum-Analyse

Beispiel: Ampelschaltung

Für die Steuerung einer Ampelanlage an einer Straßenkreuzung soll auf Basis des Architekturdesigns eine Sicherheitsanalyse durchgeführt werden. Dabei ist vor allem die Gefahrensituation zu untersuchen, dass zwei Autos zusammenstoßen könnten.

Die Randbedingungen für die Ampelanlage sind die folgenden (gegenüber einer realen Situation etwas vereinfachten):

- Zwei Straßen kreuzen sich;
- an jeder Eintrittsstelle befindet sich eine (Auto-)Ampel; d.h. eine Ampel mit Leuchten für Rot, Gelb und Grün
- jede Leuchte verfügt über eine redundante Auslegung, d.h. es ist ein Reserverleuchtmittel vorhanden, dass bei einem Ausfall des ersten Leuchtmittels automatisch angesteuert wird (soetwas kann auf der Ebene der elektrischen Schaltung realisiert werden). Ein Ausfall des zweiten Leuchtmittels kann über Sensoren abgefragt werden.

Die Aufgabe der zentralen Steueranlage für die Kreuzung ist das geregelte Schalten der Ampeln, sowie das Erkennen von und reagieren auf Fehlersituationen. Die Schnittstellen zu den Ampeln sind Sensoren und Aktuatoren, die den Status der Leuchten liefern bzw. neu setzen. Für die Regelung des Ablaufs werden Timer verwendet, die geeignet vorbesetzt sind.

Der Steuermechanismus soll für jede einzelne Ampel folgendes realisieren:

- Bei der Initialisierung soll die Ampel auf Rot geschaltet werden.
- Die Abfolge der Ampelsignale ist “ROT - GRÜN” bei Freigabe der Fahrtrichtung und “GRÜN - GELB - ROT” bei Sperren der Fahrrichtung. Dabei werden für die Übergänge eigene Timer verwendet um die Dauer der jeweiligen Leuchtenphasen zu regeln.

Darüberhinaus müssen die gegenüberliegenden Ampeln synchronisiert werden.

Die Sicherheitsanalyse soll auf Basis dieser Beschreibung aufgesetzt werden; zusätzliche Designentscheidungen können im Laufe der Analyse hinzugenommen werden, falls dies notwendig ist.