

Abschlussbericht der Studie

Fehlertolerante Systeme

- Prinzipien und Ausführungsbeispiele -

Fehlertoleranz spielt nicht nur bei hoch sicherheitskritischen Systemen wie beispielsweise elektrische Flugsteuersysteme (Fly-by-Wire) oder die Sicherheitssysteme in Kernkraftwerken eine bedeutende Rolle, sondern gewinnt auch in vielen anderen Bereichen (z.B. Fahrzeugtechnik, Bussysteme etc.) zunehmend an Bedeutung. Aufgrund der steigenden Anzahl an Komponenten und der zunehmenden Komplexität sinkt die Zuverlässigkeit des Gesamtsystems. Bei mechanischen, pneumatischen und hydraulischen Komponenten kann mit Hilfe des traditionellen Ansatzes der Perfektion (Überdimensionierung, verbesserte Materialien, umfangreiche Qualitätskontrollen etc.) die Ausfallwahrscheinlichkeit verringert werden. Bei elektrischen, elektronischen und elektronisch programmierbaren Systemen (E/E/EP Systeme nach IEC 61508) hingegen sind diesem traditionellen Ansatz Grenzen gesetzt. Bei dem Ansatz der Toleranz wird hingegen der Ausfall einzelner Komponenten berücksichtigt und die Funktionsfähigkeit des Gesamtsystems durch entsprechende Massnahmen im Fehlerfall (Umschalten auf redundante Komponenten, Rekonfiguration etc.) vollständig oder vermindert gewährleistet.

In den ersten Abschnitten der Studie (Theorieteil) werden Definitionen, Richtlinien und Normen sowie Redundanzkonzepte, die für fehlertolerante Systeme von Bedeutung sind, vorgestellt. Anhand von Praxisbeispielen und Beispielen aus Entwicklungs- und Forschungsarbeiten werden in den darauf folgenden Abschnitten konkrete Realisierungen von fehlertoleranten Systemen untersucht.

Berichtsumfang: 146 Seiten
Dauer der Studie: 01.04.2007 - 31.07.2007
Zuschussgeber: DFAM
Forschungsstelle: Technische Universität Darmstadt
Institut für Automatisierungstechnik
Forschungsgruppe Regelungstechnik und Prozessautomatisierung
Prof. Dr.-Ing. Dr. h.c. Rolf Isermann
Landgraf-Georg-Straße 4
64283 Darmstadt
Bearbeiter/Verfasser: Dipl.-Ing. M. Beck