

Software-Based Redundancy Techniques for High-Reliability Embedded Real-Time Systems

Martin Hoffmann Peter Ulbrich Wolfgang Schröder-Preikschat

Friedrich-Alexander-Universität Erlangen-Nürnberg

Moderne Prozessoren werden durch steigende Transistordichte und niedrigere Versorgungsspannungen immer anfälliger für externe physikalische Einflüsse, wie elektromagnetische Strahlung oder hochenergetische Partikel. Diese können zu transienten Hardwarefehlern führen und den Zustand und damit das Verhalten eines Rechensystems drastisch beeinflussen.

Aktuelle Serversysteme nutzen fehlerkorrigierende Codes für Arbeitsspeicher und Caches um transienten Fehlern entgegenzutreten. Dennoch tauchen in den letzten Jahren zunehmend Meldungen von Abstürzen einzelner Knoten aufgrund von “Soft Errors” auf.

Auf der anderen Seite stehen eingebettete Rechensysteme, mit teilweise erheblich strengeren Zuverlässigkeitsanforderungen. Vor allem im Luftfahrtbereich wird deshalb echte Hardwareredundanz eingesetzt, um die geforderten Sicherheitsstandards zu gewährleisten. Diese Vorgehensweise ist jedoch nicht auf alle Einsatzszenarien eingebetteter Systeme anwendbar, da gerade in diesem Bereich Kosten, Energieverbrauch und Gewicht einen entscheidenden Faktor darstellen. Ein weiterer Aspekt ist der Einzug mehrkerniger Prozessoren in die Welt der eingebetteten Systeme, welche es ermöglichen verschiedene kritische und unkritische Aufgaben auf ein einzelnes System zusammen zu führen und damit die Kosteneffektivität weiter zu optimieren. Softwarebasierte Redundanztechniken können die Zuverlässigkeit solcher Systeme erhöhen ohne zusätzliche Hardwarekosten zu verursachen.

Im Vortrag wird der CoRed (Combined Redundancy) Ansatz vorgestellt, der verschiedene softwarebasierte Redundanztechniken kombiniert, um einen umfassenden Schutz der Verarbeitungskette eines typischen eingebetteten Systems (Sensordatenerfassung, Verarbeitung, Aktuatorstellung) zu gewährleisten. CoRed lässt sich generisch in ein komponentenbasiertes Echtzeitsystem eingliedern und ermöglicht somit eine selektive Redundanzenerweiterung, die sich auf sicherheitskritische Softwarekomponenten beschränken kann und gleichzeitig unkritische Anwendungen integriert. Der CoRed Ansatz wurde konkret umgesetzt und wird in einem Modellquadropter erfolgreich eingesetzt.