

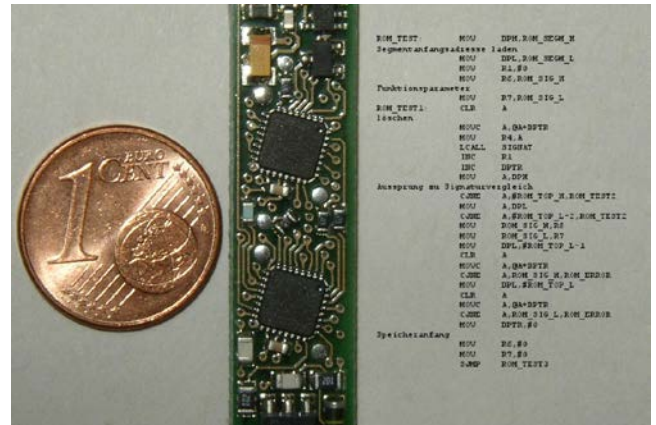
## Selbsttests für Mikroprozessoren mit Sicherheitsaufgaben

### Problem

Maschinen mit Mikroprozessorsteuerungen sind aus dem heutigen Arbeitsalltag nicht mehr wegzudenken. Zunehmend übernehmen solche Steuerungen auch Sicherheitsfunktionen und gerade komplexe Sicherheitsfunktionen sind ohne den Einsatz von Mikroprozessoren oft nicht denkbar.

Parallel zur fortschreitenden technischen Entwicklung wurden auch die relevanten Normen angepasst. Sie unterliegen noch immer einem fortschreitenden Prozess, um diese kontinuierliche Entwicklung sicherheitstechnisch zu begleiten. Im Unterschied zu Geräten des täglichen Umgangs (Wer kennt nicht die Weiterentwicklung vom Kassettenrecorder hin zum MP3-Player?) sind an Maschinen und Anlagen erhöhte Anforderungen für das sichere und unfallfreie Arbeiten zu definieren. Diesen Umstand berücksichtigen auch die Normen für die neuen Mikroprozessoren. Neben Anforderungen an die Struktur einer Maschinensteuerung werden auch Anforderungen an die Organisation gestellt und dezidierte Aussagen zur Gestaltung von Software getroffen.

Trotz dieser Beschreibung der in der Software zu treffenden Maßnahmen ist die konkrete Umsetzung nicht einfach. Aus Sicht des IFA bedarf es oft nur eines kleinen Beispiels, damit diejenigen, die Software entwickeln, selbst eine bedarfsgerechte Lösung für die eigene Anwendung finden.



Sichere Software hängt nicht von der Größe der Rechner ab

### Aktivitäten

Um für Beratungen und Anfragen geeignete Beispiele für automatische Rechner selbsttests anbieten zu können, wurden im IFA eigene Routinen für einen Mikrocontroller des Typs 80C537 entwickelt, modular programmiert und kommentiert. Dabei wurde auf unbedingte Unabhängigkeit von bereits bestehenden Lösungen geachtet und die Software nur auf der Basis der relevanten Normen erarbeitet. Eine Prüfung der entstandenen Softwaremodule erfolgte nach den Maßstäben einer Softwareprüfung, wiederum nach den Vorgaben der Normen.

### Ergebnisse und Verwendung

Die erläuternde Beschreibung der Softwaremodule wurde in einem BGIA-Report veröffentlicht, dieser steht im Internet zum Download zur Verfügung.

Die Softwaremodule sind in einem Archivfile zusammengefasst und können ebenfalls kostenlos heruntergeladen werden.

Bei der Programmierung wurde vermieden, von den besonderen Hardwareeigenschaften des Rechners Gebrauch zu machen. Somit sollten die Tests ohne große Schwierigkeiten auf andere Mikroprozessoren übertragbar sein. Sollte dies im Einzelfall dennoch nicht gelingen, so stellen die Beispiele zumindest eine Anregung dafür dar, wie die Anforderungen der Normen in die Praxis umsetzbar sein könnten.

### **Nutzerkreis**

Alle, die Software für sicherheitsrelevante Systeme entwickeln

### **Weiterführende Informationen**

- Selbsttests für Mikroprozessoren mit Sicherheitsaufgaben oder: „Quo vadis Fehler“? BGIA-Report 7/2006. Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2006, [www.dguv.de/webcode/d6163](http://www.dguv.de/webcode/d6163)
- DIN EN 61508 Teile 1-7: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme. Beuth, Berlin 2011
- DIN EN ISO 13849-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen. Teil 1: Allgemeine Gestaltungsleitsätze (12.08). Beuth, Berlin 2008

### **Fachliche Anfragen**

IFA, Fachbereich 5: Unfallverhütung – Produktsicherheit

### **Literaturanfragen**

IFA, Zentralbereich