embeX
Your embedded experts

Herzlich Willkommen!

Mikrocontroller

in sicherheitsbezogenen Anwendungen

Martin Lange
embeX GmbH

Die embeX GmbH

- Dienstleister für die Entwicklung von embedded Systemen
- Hardware, Software, Firmware
- von der Idee bis zur Serie
- gegründet 2001 in Freiburg im Breisgau
- ca. 140 Mitarbeiter
- seit über 12 Jahren Entwicklung von sicheren Komponenten
- in: Medizintechnik, Industrieautomatisierung, Avionik, Railway

Übersicht

1. Fehlerbetrachtung in der Medizintechnik und in Industrieanwendungen
2. Prozessorinterne Fehler
3. Prozessorexterne Fehler
4. Selbsttestbibliotheken
5. Sicherheitsprozessoren

Fehlerbetrachtung

- Medizintechnik (IEC 60601-1)
  - Fehlerbetrachtung aus Risikoanalyse
  - Erstfehlersicherheit (nach IEC 60601-1, ed.3):
    wenn der erste Fehler „bevor eine zweite Maßnahme (…) ausfällt, festgestellt wird …“

- Automatisierung (IEC 61508)
  - Probabilistischer Ansatz
  - ab einem best. Risiko: zweikanalige Strukturen vorgeschrieben
  - z.B. Kat. 3 nach ISO 13849-1: „… müssen so gestaltet werden, dass ein einzelner Fehler (…) nicht zum Verlust der Sicherheitsfunktion führt. Wenn immer in angemessener Weise durchführbar, muss ein einzelner Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden.“

Fehlerbetrachtung für Mikroprozessoren

- wenn ein Mikroprozessor (allein) ein Risiko mindert / eine Sicherheitsfunktion ausführt
  - dann muss ein Fehler im Prozessor erkannt werden, bevor das Risiko zu einer tatsächlichen Gefährdung führen kann
  - Diagnosezeit ergibt sich aus der Risikoanalyse

- wenn zwei Mikroprozessoren (redundant) ein Risiko mindern / eine Sicherheitsfunktion ausführen
  - dann muss ein Fehler im ersten Prozessor erkannt werden, bevor ein Fehler im zweiten Prozessor auftritt
  - Diagnosezeit?

- Automatisierung (IEC 61508)
  - abhängig vom Risiko: Forderung eines bestimmten Diagnose-deckungsgrads (*diagnostic coverage - DC*)
  - normative Festlegung des DC für best. Diagnosemechanismen

Tabelle A.9 – Energieversorgung

Diagnoseverfahren/Maßnahme	Siehe IEC 61508-7	Als höchstens erreichbar betrachteter Diagnosedeckungsgrad	Anmerkungen
Überspannungsschutz mit Sicherheits-abschaltung oder Umschaltung auf zweite Energieversorgung	A.8.1	Niedrig	
Spannungsüberwachung (sekundär-seitig) mit Sicherheitsabschaltung oder Umschaltung auf zweite Energie-versorgung	A.8.2	Hoch	
Energieabschaltung mit Sicherheits-abschaltung oder Umschaltung auf zweite Energieversorgung	A.8.3	Hoch	

(IEC 61508, Teil 2, Anhang A)

Übersicht

1. Fehlerbetrachtung in der Medizintechnik und in Industrieanwendungen
2. Prozessorinterne Fehler
3. Prozessorexterne Fehler
4. Selbsttestbibliotheken
5. Sicherheitsprozessoren

Speicherfehler

Diagnosemechanismen

- Programmspeicher
  - min. 16-Bit-CRC (DC hoch)
- Arbeitsspeicher (stuck-at, Kurzschlüsse)
  - Galpat-Test (DC hoch)
  - Ausführungszeit quadratisch mit der Speichergröße
    → für einkanalige Anwendungen kaum geeignet
- Arbeitsspeicher (soft-errors)
  - Datensicherung (inverse Redundanz oder CRC)

Speicherfehler (Fortsetzung)

Diagnosemechanismen

- Special Function Register (SFRs)
  - Zyklischer Abgleich mit Sollwert
  - Auch für nicht verwendete Peripherie
    - ➔ Aufwand steigt mit der Komplexität des Prozessors

Diagnosemechanismen

- Fehler der Recheneinheit
  - Zyklischer Test der Maschinenbefehle
    - ➔ Aufwand steigt mit der Komplexität des Prozessors

I/O-Fehler

Diagnosemechanismen

- Fehler in Ein-/Ausgangspins
  - Dynamisierung
  - Rücklesung
  - Zweikanaligkeit

Weitere Fehler

- Fehler in der MMU
- Fehler im Cache
- Fehler in …

➔ Aufwand steigt mit der Komplexität des Prozessors

Übersicht

1. Fehlerbetrachtung in der Medizintechnik und in Industrieanwendungen
2. Prozessorinterne Fehler
3. Prozessorexterne Fehler
4. Selbsttestbibliotheken
5. Sicherheitsprozessoren

Prozessorexterne Fehler

- Fehler in der Umgebung
  - Über-/Unterspannung
  - Über-/Untertemperatur
  - Über-/Untertaktung

➔ nicht vorhersagbares Verhalten

Prozessorexterne Fehler

Diagnose

- Über-/Unterspannung
  - schnelle Änderung
  - externe Überwachung
- Über-/Untertemperatur
  - langsame Änderung
  - ggf. interne Überwachung
- Über-/Untertaktung
  - schnelle Änderung
  - externe Überwachung (z.B. Vergleich zwischen zwei Prozessoren)
  - Vorsicht bei maximaler Taktfrequenz!

Übersicht

1. Fehlerbetrachtung in der Medizintechnik und in Industrieanwendungen
2. Prozessorinterne Fehler
3. Prozessorexterne Fehler
4. Selbsttestbibliotheken
5. Sicherheitsprozessoren

Selbsttestbibliotheken

- Vorteile
  - Reduzierung des Entwicklungsaufwands
  - Reduzierung des Entwicklungsrisikos
  - Ich muss mich nicht mit den Details des Prozessors beschäftigen

- aber:
  - Welche Prozessorfehler sind wirklich abgedeckt?
    - Auch Fehler in typspezifischen Komponenten (z.B. Cache, MMU)?
  - Erfüllt die Bibliothek meine Timing-Anforderungen?
  - Was ist mit Power-Up-Tests?
  - Entspricht die Bibliothek den Anforderungen der IEC 62304?

Übersicht

1. Fehlerbetrachtung in der Medizintechnik und in Industrieanwendungen
2. Prozessorinterne Fehler
3. Prozessorexterne Fehler
4. Selbsttestbibliotheken
5. Sicherheitsprozessoren

Sicherheitsprozessoren

Was bietet der Markt aktuell an?

- Zertifizierte Prozessoren ohne Sicherheitsarchitektur
- Prozessoren mit sicherer Kernarchitektur (dual-core Lockstep-Prozessoren)
- Prozessoren mit sicherer Architektur der Kerne und der Peripherie

Zertifizierte Prozessoren ohne Sicherheitsarchitektur

Standardprozessorarchitektur (einkanalig)

- Vorteile
  - Integrierte Sicherheitsmechanismen wie Speicherabsicherung
  - Zertifizierte SW-Bibliothek für Selbsttests und Konfiguration der Prozessor-HW

- aber:
  - In der Industrieautomatisierung bietet der Einsatz eines zertifizierten Prozessors ohne Sicherheitsarchitektur derzeit keinen Vorteil bei der Zertifizierung einer Sicherheitsanwendung.
  - Einsatz in Kat. 3-Anwendungen (Erstfehlersicherheit) fraglich

Prozessoren mit sicherer Kernarchitektur

Zwei Prozessorkerne im Lock-Step-Mode
Keine sichere Peripherie

- Vorteile
  - kontinuierliche und vollständige Überwachung der Recheneinheit zur Laufzeit
  - Synchronisation zwischen zwei Prozessoren in SW nicht erforderlich
  - Einsatz in Kat. 3-Anwendungen (Erstfehlersicherheit) möglich

- aber:
  - HW-Zugriffe nicht sicherer als mit Standardprozessoren
  - Zertifizierungssituation nicht immer klar

Prozessoren mit sicherer Architektur und der Peripherie

Zwei Prozessorkerne im Lock-Step-Mode
Zweikanalige rückwirkungsfreie Peripherie

- Vorteile
  - kontinuierliche und vollständige Überwachung der Recheneinheit zur Laufzeit
  - Synchronisation zwischen zwei Prozessoren in SW nicht erforderlich
  - Einsatz in Kat. 3-Anwendungen (Erstfehlersicherheit) möglich
  - sichere (zweikanalige) HW-Zugriffe möglich
- aber:
  - ---

Kriterienliste (1)

- Welchen Beitrag zur Risikoreduktion muss der Prozessor in meiner Anwendung leisten:
  - Steuerung einer risikobehafteten Funktion (erstfehlersicher) oder
  - nur Überwachung („zweite Maßnahme“)?
- Muss der Prozessor in meiner Anwendung Hardware sicher ansteuern oder dient er nur als „Rechner“?
- Werden alle benötigten Komponenten des Prozessors durch die (in SW oder HW) integrierte Diagnosefunktionen abgedeckt.
  - mit welcher Wirksamkeit?
  - Werden dafür Power-Up-Tests in Anspruch genommen, obwohl mein Gerät für Dauerbetrieb vorgesehen ist?
- Ist die Performance des Sicherheitsprozessors ausreichend (derzeit: < ca. 350 MHz)?

Kriterienliste (2)

- Ist die Architektur des Prozessors zertifiziert?
- Erfüllt die dazu angebotene Safety-Software die IEC 62304?
- Bin ich bereit, mögliche Nachteile in Kauf zu nehmen:
  - höhere Komplexität?
  - Single Source?
  - vergleichsweise neue Technologie?
  - höherer Preis?

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Martin Lange
Leiter Geschäftsbereich
Safety in Automation
embeX GmbH
Heinrich-von-Stephan-Straße 23
D-79100 Freiburg

Tel.: +49 (0)761 - 47 97 99 - 14
m.lange@embeX.de
www.embex.de