Softwareengineering für Sicherheitssysteme

Florian Pitzl

12. November 2012

Inhaltsverzeichnis

Einleitung

Normale Entwicklung

Eine gegeben Funktion erfüllen

Entwicklung sicherheitsgerichtete Systeme

Nicht nur geforderte Funktion realisieren, sondern auch sicherstellen, dass die Lösung immer richtig „funktioniert“

In der Sicherheitstechnik ist ein verantwortungsbewusstes Handeln notwendig!

Wichtige Normen und Einstufungen

Relevante Normen

Norm	**Anwendungsbereich**
DIN EN61508	„Grundnorm“, u.a. Maschinenbau
RTCA DO178B	Luftfahrt
DIN EN60601	Medizintechnik

Einstufungen nach EN61508

SIL	**Folgen bei Versagen**	**Gefährlicher Ausfall nach [Jahre]**
SIL1	Kleine Schäden an Anlagen und Eigentum	10
SIL2	Große Schäden an Anlagen, Personenverletzung	100
SIL3	Verletzung von Personen, einige Tote	1000
SIL4	Katastrophen, viele Tote und gravierende Umweltverschmutzung	10000

Die notwendige Einstufung erfolgt anhand der Eintrittswahrscheinlichkeit und den möglichen Folgen. Die erreichte Einstufung ergibt sich aus der Fehlerbetrachtung.

Fehlerbetrachtung

Theorem

Es gibt kein System ohne Fehler. Die Eintrittswahrscheinlichkeit kann aber durch geeignete Maßnahmen begrenzt werden.

Ziel der Entwicklung ist es, die gefährlichen, nicht aufdeckbaren Fehler auf den nach der Risikoanalyse notwendigen SIL-Grad zu begrenzen.

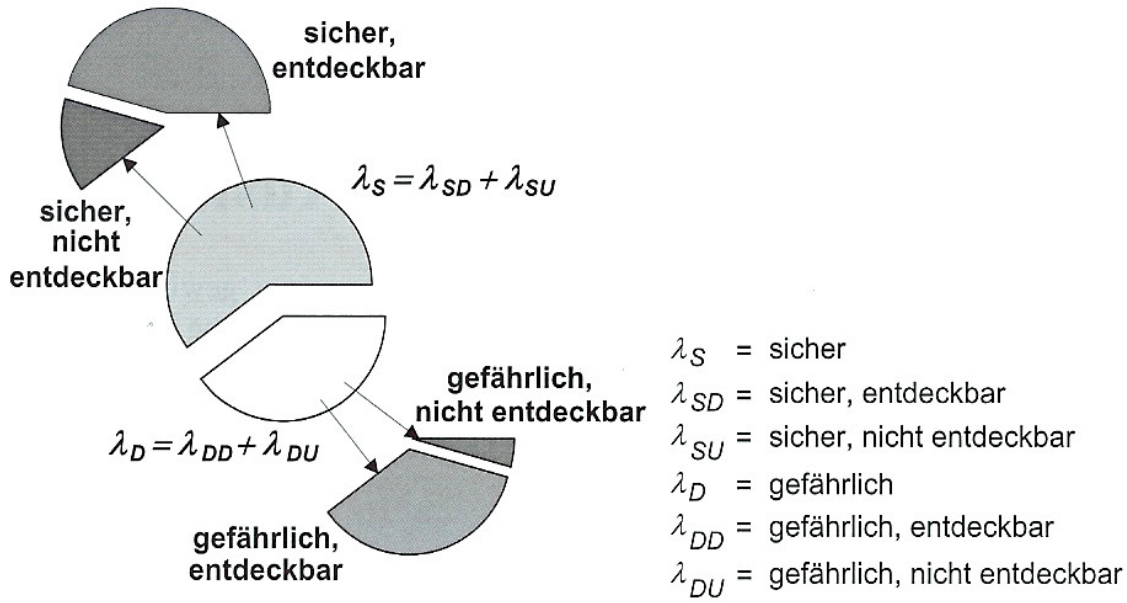

Bild 4.1: Fehlerraten

Fehlerbetrachtung Hardware

In der Hardware können neben systematischen Fehlern auch stochastische Fehler auftreten. Die systematischen Fehler können durch geeignete Entwicklungsmaßnahmen weitestgehend vermieden werden. Es wird eine Analyse zur Fehlereintrittswahrscheinlichkeit und ihrer Auswirkung über Fehlermodelle wie z.B. Fehlerbaum, FMEA, etc. gemacht.

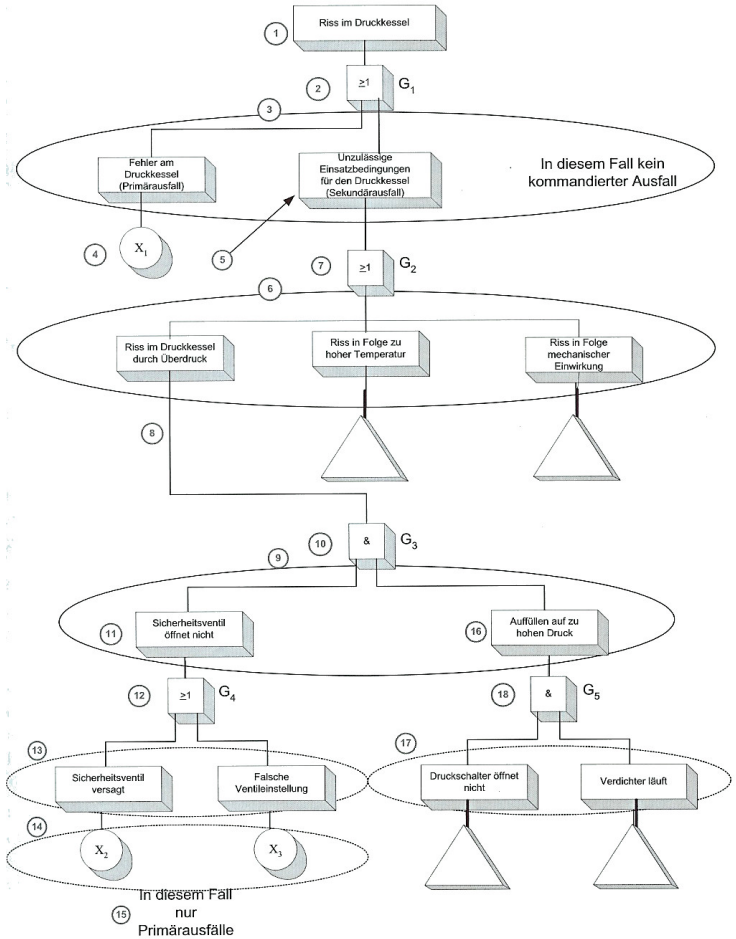

Bild 9.2: *Fehlerbaum für Ereignis „Riss im Druckkessel“*

Abbildung : *Fehlerbaum*

Fehlerbetrachtung Systemstruktur

Zur Erreichung der geforderten Ausfallsicherheit kann es notwendig sein die Systemstruktur wie folgt auszulegen:

- mit Diagnosepfad
- teilweise redundant
- redundant
- teilweise diversitär
- diversitär

```
if(!comCopy((uint8_t*)&ownTime.syncId, (uint8_t*)&otherTime,
(uint8_t)(sizeof(ownTime)), TIMEOUT_SHORT))
{
setError(ERR_CYCLE_TIME, TYPE_FATAL);
}
else if (otherTime.syncId != syncId.cycleTimeSyncId)
{
setError(ERR_CYCLE_TIME_SYNC_ID, TYPE_FATAL);
}
else if (ownTime.time != otherTime.time)
{
setError(ERR_CYCLE_TIME_DIFF, TYPE_FATAL);
}
...
```

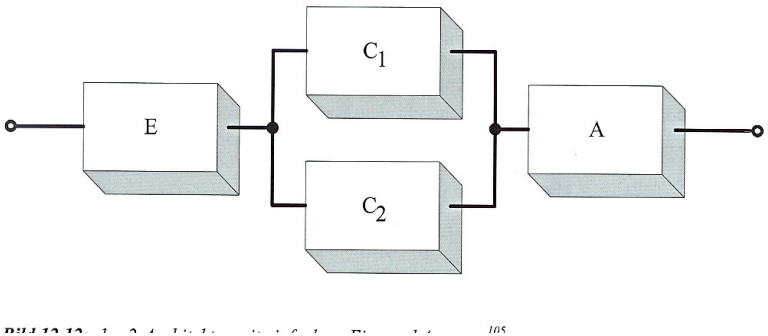

Abbildung : *1oo2 Systemstruktur*

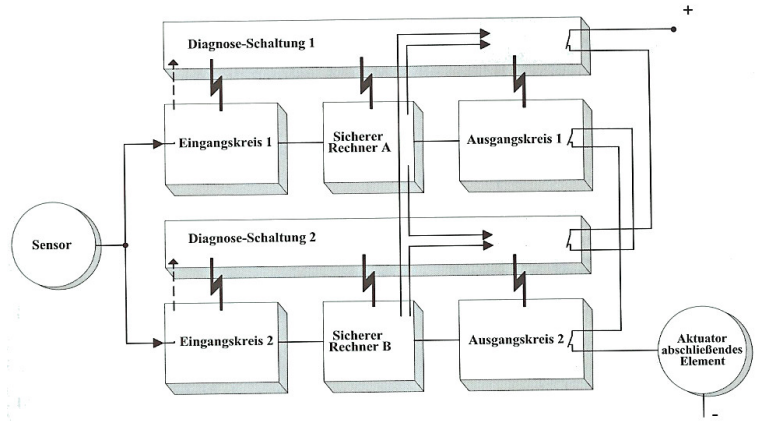

Abbildung : *1oo2D Systemstruktur*

Fehlerbetrachtung Software

In der Software können nur systematische Fehler vorkommen. Diese werden durch entsprechende Entwicklungsabläufe so weit wie möglich vermieden.

In der Regel muss die Software auch Maßnahmen beinhalten um Hardwarefehler aufzudecken.
z.B. Maßnahmen für Stuck-At-0 in Speicherzelle:

- Ramtest
- Redundante Datenhaltung
- Diversitäre Datenhaltung
- Blockinverse Datenhaltung

Ablauf Softwareentwicklung

Die Normen fordern die Einhaltung und Verwendung formaler Entwicklungsmethoden wie z.B. dem V-Model. Dieser Prozess wird durch externe Zertifizierungsstellen wie z.B. dem TÜV-Süd überwacht.

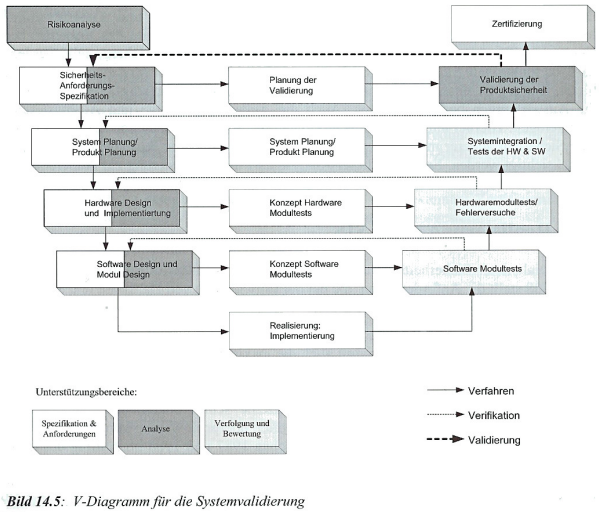

Bild 14.5: V-Diagramm für die Systemvalidierung

Abbildung : *V-Model*

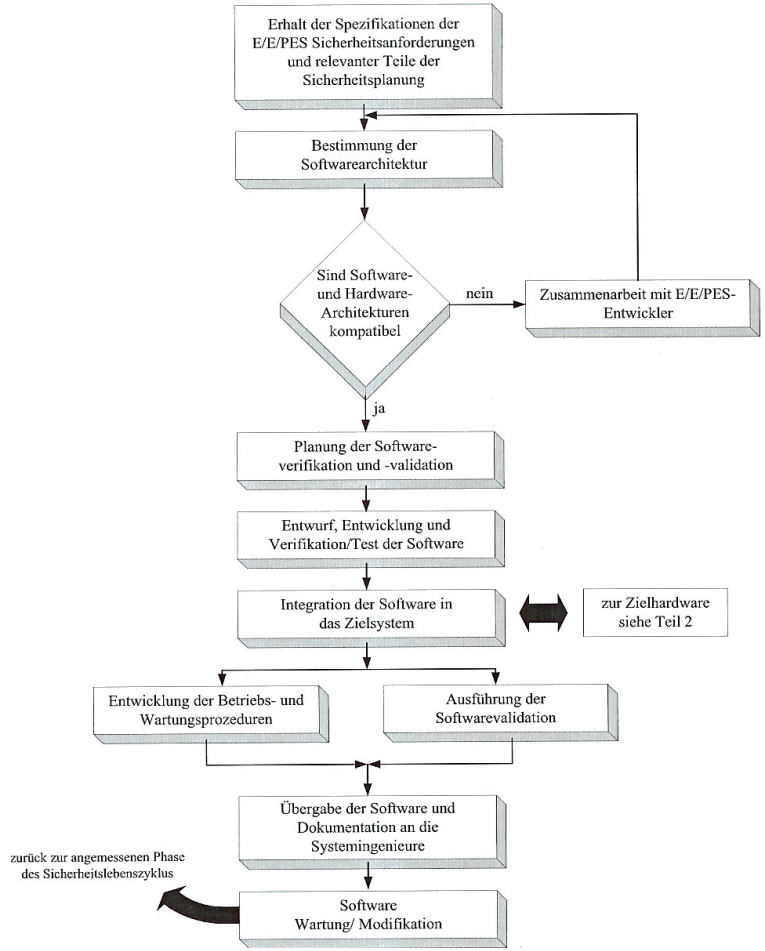

Abbildung : *Ablauf nach EN61508*

Entwicklungstechniken Softwareentwicklung

Anforderungen - je nach SIL

- Programmierrichtlinen (z.B. MISRA)
- Eingeschränkter Sprachumfang (C/C++)
- Defensive Programmierung
- Testdriven development

```
uint8_t Dis_itoa(uint16_t val, char_t *pBuffer, uint8_t size)
{
static uint8_t retVal;

retVal = (uint8_t)ERR_NO_ERROR;

if (size == (uint8_t)0U)
{
retVal = (uint8_t)ERR_DIS_PAR_INVALID;
}
else if (pBuffer == NULL)
{
retVal = (uint8_t)ERR_DIS_PAR_POINTER;
}
...
return retVal;
```

Prüfungen je nach Kritikalität

- Review durch SW-Walkthrough
- SW-Modultest (Blackbox / Whitebox)
- SW-Integrationstests
- SW-Fehlerversuche

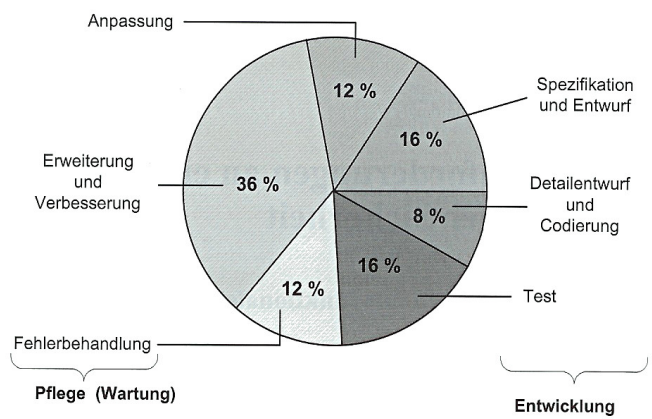

Bild 18.1: Relativer Anteil des Gesamtaufwands über die gesamte Lebensdauer eines Produktes[16]

Abbildung : *Relativer Aufwand*

Vielen Dank für die Aufmerksamkeit!

Quellen

- VDE, DIN EN61508, 2001
- Josef Börcsök, Funktionale Sicherheit, 2008, ISBN 978-3-7785-4051-0