Konzeption sicherer Systeme

Unser tägliches Leben ist geprägt durch Maschinen, denen wir blind unser Leben anvertrauen. Sie stellen oftmals eine potentielle Gefahr dar und können zu Katastrophen führen, die es ohne sie nicht geben würde. Um sich vor diesen Gefahren zu schützen, werden wiederum technische Mittel eingesetzt, die ebenfalls ein Risiko in sich bergen. Durch diese kann die Anlage beim Nutzer noch mehr Vertrauen erlangen, und um so schlimmer ist dann eine Fehlfunktion, mit der keiner gerechnet hat.

Bei der Entwicklung sicherheitsrelevanter Systeme, deren Versagen tödliche Folgen haben kann, ist die Frage: *Wann ist das System sicher genug?* nicht beantwortbar. Wünschenswert wäre es, alles menschen-mögliche für die Sicherheit zu tun. Die Sicherheit einer Anlage baut auf zwei Aspekten auf: 1. Die Entwicklung war korrekt, so daß das System macht, was es machen soll. 2. Die Laufzeitfehler, Ausfälle und Ausnahmen (z.B. aus der Hardware, Mechanik und/oder Bedienung) werden erkannt und richtig behandelt. Um ein sichereres System zu konzipieren, ist es empfehlenswert, es zu vereinfachen, die Interaktion Mensch-Maschine zu überdenken, Gefahren zu erkennen und Maßnahmen für die Gefahrenbeherrschung zu planen. (Sie können weitere Informationen zu diesen Themen unter
http://www.first.gmd.de/~sergio/public finden).

Vereinfachen

Wenn die Komplexität eines Systems steigt, sinken seine Sicherheit und seine Verfügbarkeit, da ein Versagen jeder Komponente das Versagen des Gesamtsystems bedeuten kann, die Entwicklung wird unübersichtlicher und die Anzahl der Schnittstellen (Schwachstellen und Fehlerquellen) steigt.

Kooperation Mensch-Maschine

Es gibt eine Tendenz, Sicherheit durch Automatisierung zu erreichen. Bei 80% der Flugzeugkatastrophen lautet der Befund “Menschliches Versagen”. Leider gibt es keine Statistik, wie oft Piloten ein Versagen der Technik beherrschen mußten, um eine Katastrophe zu vermeiden. Diese Zahl dürfte aber höher als die erste sein. Bei der zunehmenden rechnergestützten Kontrolle eines gesamten Systems rücken Rechner und Software mehr und mehr auf einen sicherheitsrelevanten (kritischen) Platz. Es gibt fünf Stufen dieser Rechnerintegration :

1. Rechner werden eingesetzt, um Benutzern auf Anfrage Informationen zu liefern.

2. Der Rechner interpretiert Daten und schlägt Handlungen vor. Der Benutzer entscheidet und handelt.

3. Der Rechner steuert direkt das technische System. Der Benutzer überwacht ihn und kann notfalls Maßnahmen ergreifen.

4. Der Mensch wird aus der Kontrollschleife entfernt, wodurch Rechnersteuerung und technisches System ohne menschliche Hilfe oder Wirkung selbständig arbeiten.

5. Der Rechner kann (darf) menschliche Anweisungen ignorieren (sogar im Störfall).

Sergio Montenegro, GMD-FIRST, Rudower Chaussee 5, D-12489 Berlin-Adlershof
Tel +49/30/6392-1878, email: sergio@first.gmd.de

Es sollte viel lieber ein Team Mensch-Maschine gebildet werden, wo beide Parteien miteinander kooperieren und sich ergänzen. Die Maschine kann besser schnell regeln als der Mensch, aber für die Behandlung von Ausnahmen und unvorhersehbaren Situationen ist der Mensch mit seiner Kreativität und Intuition weit überlegen. Bei der Interaktion Mensch-Maschine sollte jeder in der Lage sein, Fehler des anderen (Mensch: Bedienungsfehler; Maschine: echt dumme Fehler) abzufangen und zu korrigieren.

Risiken und Gefahren erkennen

Der "normale" Funktionsbereich eines Systems ist ein sehr schmales Band, der Fehlerbereich dagegen der Rest. Ein kleiner Fehler oder eine unvorhersehbare Situation kann das System in den "Fehlerbereich" bringen. In der Regel werden diese Umstände erst erkannt, nachdem sie (negative) Folgen (oder gar einen Unfall) verursacht haben.

Dies ist besonders bei Software-, Bedienungs- und Kommunikationsfehlern der Fall. Je früher deren Eintreten erkannt wird, desto weicher und effektiver können die Maßnahmen sein. Daher ist es ratsam, Redundanz und Prüfmechanismen (Plausibilitätsprüfungen) vorzusehen. Um die Gefahren zu erkennen, hilft nur der gesunde Menschenverstand, unterstützt von einigen Hilfstechniken: Definition gefährlicher Situationen, hazard analysis, Checklisten, fault tree analysis, event tree analysis und FMEA: Fehlerminimierung und Einflußanalyse.
[**http://www.first.gmd.de/~sergio/seminar**]

Alle gefundenen Gefahren sollten ernst genommen werden. Oft wird der Fehler gemacht, daß eine so kleine Wahrscheinlichkeit für das Auftreten einer Gefahr berechnet wird, daß diese nicht weiter verfolgt wird. Dabei werden die möglichen Konsequenzen ignoriert, obwohl sie sehr groß sein können. Sehr oft geschah genau das bei großen Katastrophen. Die Wahrscheinlichkeit war so niedrig, daß keine Maßnahmen für den Notfall bereit waren. Klassisches Beispiel: Die Titanic hatte zu wenige Rettungsboote, weil sie "unsinkbar" war.

Gefahren beherrschen

Das Risiko kann man nicht ausschalten, man muß damit leben (oder sterben). Aber man sollte es mindestens beherrschen können und einen Ausweg vorbereitet haben. Dazu werden folgenden Prioritäten empfohlen: 1. Gefahrenstellen vermeiden oder eliminieren. 2. Die Wahrscheinlichkeit eines Unfalls minimieren. 3. Maßnahmen vorbereiten, um aus gefährlichen Situationen herauszukommen. 4. Für jeden möglichen Unfall Konsequenzen minimieren und Schäden begrenzen. Aber Vorsicht: Die Sicherheitsmaßnahmen können neue Gefahren mit sich bringen. Die neuen Elemente erfordern eine neue Gefahrenanalyse.

Sergio Montenegro, GMD-FIRST, Rudower Chaussee 5, D-12489 Berlin-Adlershof
Tel +49/30/6392-1878, email: sergio@first.gmd.de