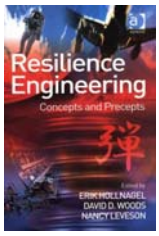
Buchrezension: „Resilience Engineering“

SIBYLLE PEUKER

Institut für Multimediale und Interaktive Systeme, Universität zu Lübeck



Erik Hollnagel, David D. Woods und Nancy Leveson (Hrsg.)
Resilience Engineering. Concepts and Precepts
Ashgate Publishing Ltd., 2006.
ISBN: 0-7546-4641-6

Der Begriff Resilience Engineering charakterisiert eine neue Art und Weise, Sicherheit in sicherheitskritische Systeme „einzubauen“. Während konventionelle Ansätze dominiert sind von Unfallanalysen, Katalogisierung von Fehlern und probabilistischen Risikoanalysen, versucht Resilience Engineering die Fähigkeit einer Organisation zu erhöhen, Prozesse robust und flexibel zu gestalten und Probleme proaktiv bei laufender Produktion und ökonomischem Druck anzugehen. Traditionelle Methoden konzentrieren sich also eher auf die Schwächen des Systems, während Resilience Engineering versucht, die Stärken auszunutzen.

Das Buch „Resilience Engineering“, herausgegeben von Erik Hollnagel, David D. Woods und Nancy Leveson, entstand im Anschluss an ein Symposium im Oktober 2004 in Schweden zu diesem Thema. Wissenschaftler verschiedener international anerkannter Forschergruppen hatten unabhängig voneinander begonnen an ähnlichen Problemen mit ähnlichen Ideen zu forschen und trafen sich in Schweden, um eine gemeinsame vorläufige Definition von Resilience Engineering festzulegen.

Resilienz ist seit längerem ein Forschungsfeld der positiven Psychologie, das sich mit der Frage beschäftigt, warum einige Menschen Lebenskrisen wie schwere Krankheiten, Arbeitslosigkeit oder Krieg und Terror ohne bleibende Beeinträchtigungen überstehen. In letzter Zeit wird der Begriff immer häufiger benutzt, um die Folgen großer Umbrüche für Organisationen und Gesellschaften zu beschreiben.

Eine Arbeitsdefinition des Begriffs Resilienz auf die sich die Autoren des Buches geeinigt haben ist diese: „Resilienz ist die Fähigkeit einer Organisation über einen signifikanten Zeitraum die Einwirkungen interner und externer Ereignisse erfolgreich auszugleichen.“

Der Ansatz des Resilience Engineering beruht nun auf zwei Annahmen: Erstens entstünden Unfälle meist durch eine Verkettung unglücklicher Umstände und selten aufgrund des Versagens einer einzelnen Komponente. Zweitens seien Fehler die notwendige Kehrseite des Erfolgs. Die Ursachen für beide lägen in der variablen Leistung des Gesamtsystems. Der Unterschied bestünde hauptsächlich darin, wie gut das System betrieben wird. Danach macht es also nicht viel Sinn, über „menschliche Fehler“ oder „menschliches Versagen“ zu reden. Stattdessen geht es in vielen Beiträgen um die Organisation, in die das (technische) System eingebettet ist.

Sicherheit sei keine Systemeigenschaft die das System ein für allemal „hat“ sondern etwas das das System „tut“. Das Dilemma ist, dass sich Sicherheit nur durch die Abwesenheit bestimmter Ereignisse zeigt. Ein Unfall bedeutet dabei nicht unbedingt, dass ein System nicht sicher ist, sondern eventuell nur, dass absolute Sicherheit nicht zu erreichen ist.

Resilience Engineering versucht also gar nicht erst, Sicherheit als eine Systemeigenschaft zu erreichen. Resilienz wird als eine bestimmte Qualität des Funktionierens gesehen. Das hat zwei Konsequenzen: Man kann nur das Potential für Resilienz messen, nicht Resilienz selbst. Man kann Resilienz auch nicht erreichen, indem man mehr Prozeduren und Barrieren einführt sondern nur, indem man ständig die Leistung des Systems überwacht. Hier fallen mir sofort die Parallelen zum Paradigmenwechsel in der Software-Entwicklung auf: Software wird immer seltener als Produkt mit endgültigen Eigenschaften ausgeliefert, sonder immer öfter als Webservice, der kontinuierlich gewartet werden muss, damit er seine Leistungsfähigkeit behält.

Das Buch ist in drei Teile gegliedert. Im ersten Teil (Emergence, Kapitel 1-7) wird Resilienz aus verschiedenen Blickwinkeln sowohl theoretisch als auch durch illustrative Beispiele beschrieben. Im zweiten Teil (Cases and Processes, Kapitel 8-16) werden Prozesse vorgestellt und an Fallbeispielen gezeigt, wie man Resilienz erreichen kann. Im dritten Teil (Challenges for a Practice of Resilience Engineering, Kapitel 17-21) wird diskutiert, wie man solche Prozesse praktisch umsetzen kann. Im Epilog werden einige immer wiederkehrende Themen noch einmal von Hollnagel und Woods zusammengefasst.

Fazit

Es gibt im Buch den Grundtenor, dass wir eine neue Herangehensweise an Sicherheit in Organisationen brauchen. Wie in einem solchen Buch zu erwarten, sind die Meinungen der Autoren zum Thema nicht völlig homogen. Die grundlegenden Prinzipien sind jedoch schon klar und die Argumente klingen fast immer logisch. Die notwendigen Methoden sind größtenteils noch zu entwickeln und zu erproben.

„So does the resilience approach offer us a paradigm shift or is it just a more positive repackaging of a century of ideas in industrial safety?” wie Rhona Flin auf Seite 233 fragt. Diese Frage wird im Buch noch nicht abschließend geklärt, aber es tendiert eindeutig zum Ersteren.

Ich selbst habe in vielen Artikeln interessante Thesen gefunden, die mich zum Nachdenken angeregt haben. Ich empfehle das Buch allen, die sich in irgendeiner Weise mit sicherheitskritischen Systemen beschäftigen. Es lohnt sich in jedem Fall, sich

von dem Buch inspirieren zu lassen, um sich selbst eine Meinung über „Resilience Engineering“ zu bilden.

Ausblick

Vom 8.-10. November 2006 fand das zweite *Symposium on Resilience Engineering* statt, das schon im Vorfeld wegen der überwältigenden Nachfrage um einen Tag verlängert wurde. Die im Buch geführte Diskussion wurde dort fortgesetzt und die diskutierten Beispiele reichen von der Katastrophe in New Orleans bis zur Fischfang-Industrie. Die Beiträge zu diesem Symposium sind unter http://www.resilience-engineering.org/proceedings.htm verfügbar.