Übungen zur Vorlesung
Safety-Critical Systems I
Sommersemester 2007

AG BS
Jan Peleska

Blatt 1

Nancy G. Leveson: A Systems-Theoretic Approach to Safety in Software-Intensive Systems

In her above mentioned article, Nancy Leveson advocates a new approach to accident analysis called STAMP (Systems-Theoretic Accident Model and Processes).
Read the introduction of this article (abstract and Section 1), in order to answer the following questions.

Aufgabe 1: Criticism with respect to conventional accident analyses (40%)

Describe at least two of the main points of criticism with respect to conventional accident analysis and the related root cause analysis Nancy Leveson outlines in her paper.

Aufgabe 2: STAMP: Leveson's new approach to accident modelling (60%)

According to Leveson's new STAMP approach to accident modelling, ...

- ... what are the most important new relationships between events to be considered ?
- ... explain Leveson's perception of safety as an emerging (*auftauchende, hervortretende*) system property.
- ... explain the notion of *constraints* in STAMP, in contrast to the focus on *events* prevailing in conventional accident analysis.
- ... explain the main aspects of *hierarchic levels of control* considered in the STAMP approach.
- ... sketch the systems theoretic approach to system control and the and how certain control flaws may lead to hazards.

Abgabe: Bis Dienstag, 08.05.2007, in der Übung.