Safety-Critical Systems I
Wintersemester 2009/10

AG BS
Jan Peleska
Florian Lapschies

Exercise 1

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

Study Nancy G. Levenson's paper "A Systems-Theoretic Approach to Safety in Software-Intensive Systems"[1] and write a two page essay discussing the following questions:

a) What is the meaning of *"Safety as an emergent system property"*?

b) Why can software never be safe?

c) Give two new examples illustrating Levesons's statement, one referring to a purely mechanical system (house, bridge, steam engine, . . .), one referring to a system controlled by embedded HW and SW.

d) Justify why it is also true that *"Security is an emergent system property"*.

e) Where are the system boundaries when analysing safety properties?

- At the system's HW interfaces?
- Or should you rather analyse the closed system consisting of HW/SW and the operational environment?

Submit your essay to `florian(at)informatik.uni-bremen.de` and hand in a printout in the session at Thursday, 5th of November.

[1] The paper is available at `http://sunnyday.mit.edu/papers/tdsc.pdf`