Prof. Dr. P. Liggesmeyer
Nikita Bhardwaj-Haupt, M.Sc.

Technical University of Kaiserslautern
Dept. of Computer Sciences
AG Software Engineering: Dependability

Safety and Reliability of Embedded Systems

SRES WS 17/18

Problem Set 1

Problem 1: Software Intensive Systems

a) Please define the general term “*System*” according to Birolini and explicitly name the parts a system can encompass. Explain your answer in the view of a technical field.
b) What is the difference to a “*Technical System*”?
c) For the analysis of a technical (embedded) system it is crucial to extract it from its environment. How can this be achieved? Please sketch your ideas.
d) Please list important non-functional requirements for embedded systems. What category (functional / non-functional) does *Safety* belong to? Why?

Problem 2: Reliability vs. Availability

Please explain the difference between “*Reliability*” and “*Availability*”.

Problem 3: Safety vs. Security

Please explain the terms “S*afety*” and “S*ecurity*”.
What is meant by “*Technical Safety*” in comparison to “*Safety*”?

Problem 4: Failure, Fault, Error

What is meant by the terms “*Failure*”, “*Fault*”, and “*Error*”? Please illustrate your answer by means of the “Ariane 5” disaster (see lecture).
Does an error always result into a failure?

Problem 5: Hardware Failures vs. Software Failures

Please explain the differences between hardware failures and software failures.

Problem 6: Correctness and Robustness

Please give your opinion on the following statements:

	true	false
Correctness has a binary character	__	__
An artifact is not consistent to its specification, if it is not correct	__	__
Robustness has a binary character	__	__
Robustness is a property only of the implementation	__	__
A safe system can suffer from security breach	__	__
Environment can influence system's safety	__	__

Problem 7: Correlation among Quality Characteristics

a) Quality characteristics might influence each other. Think about the following dependencies and figure out, whether the influences are positive or negative.

   i. Safety – Availability
   ii. Safety – Reliability
   iii. Availability – Reliability
   iv. Efficiency* – Safety/Reliability

* Within ISO 9126, efficiency is defined in terms of time and resources behavior: level of performance of a system vs. the amount of resources used.