Software Platforms for Automotive Systems

Tutorial 2: Reliability, Availability, and Safety

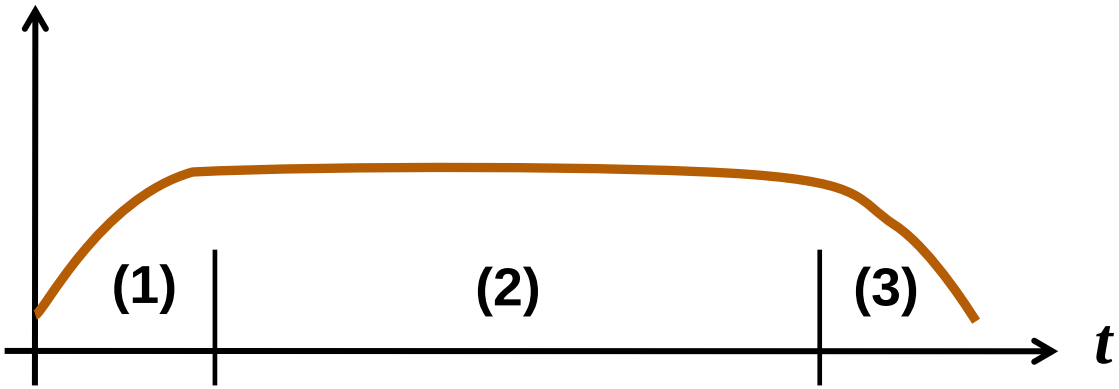
Alejandro Masrur

27th October 2015, TU Chemnitz

Failures in Automotive Systems

1) All systems, including automotive systems, might suffer from occasional failures. People usually try to predict the systems' behavior based on statistical information.

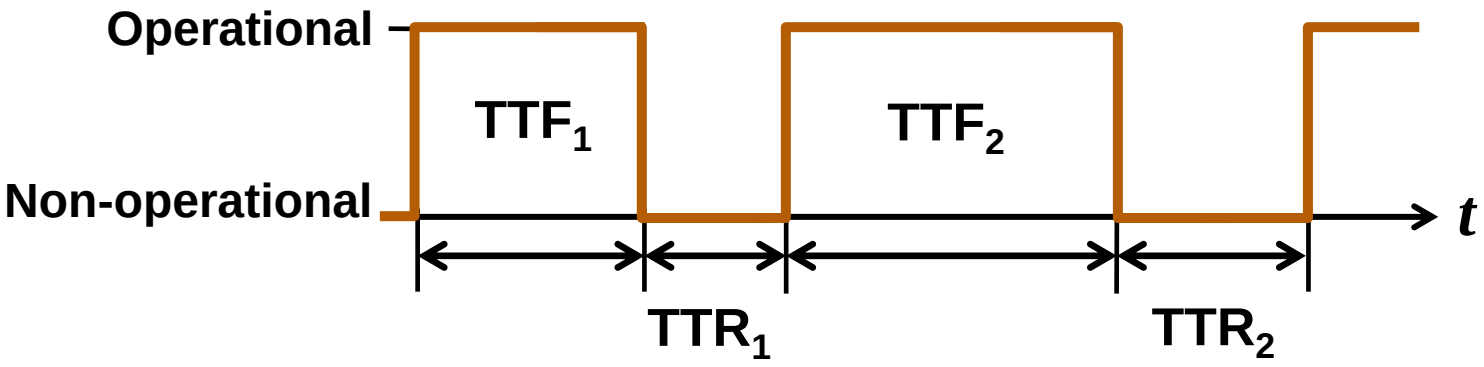
a) In this context, what does the curve below represent? What do the three different regions (1), (2) and (3) represent and what are the reasons for them?



b) What does the length of the different regions depend on? Which of these lengths can we directly influence by careful design?

MTTF and MTTR

2) It is often possible to characterize the behavior of systems (or subsystems) by two parameters as depicted below: the Time To (TTF) Failure and the Time To Repair (TTR).



a) What is the definition of MTTF and of MTTR?

b) What is the definition of failure rate and of repair rate?

c) What is the relation between MTTF and MTTR to failure and repair rate respectively?

Availability and Unavailability

3) The availability and the unavailability give the probability of a system of subsystem to be in operational or non-operational state respectively.

a) For a given system, what is the relation between availability and unavailability? Explain your answer.

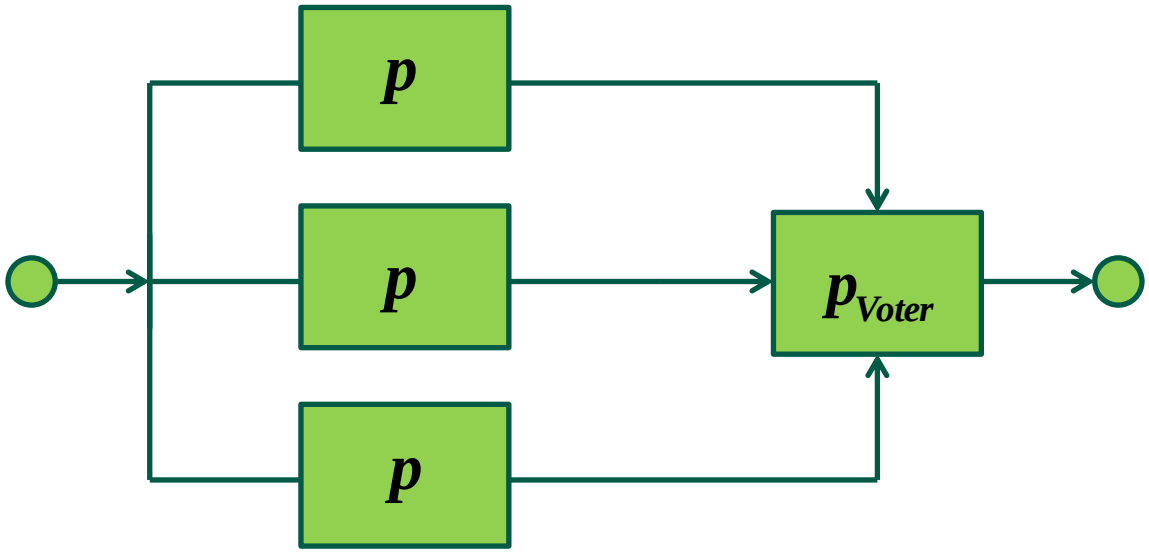
b) Is it possible to compute the availability and unavailability if we only know MTTF and MTTR of a system? Explain your answer.

c) Is it possible to compute the unavailability of a system if we only know the repair rate and the MTTF? Explain.

d) What is the relation between availability and reliability of a system? Explain your arguments.

Redundancy

4) Availability is now becoming important for automotive systems, in particular, considering new applications such as autonomous driving. Triple modular redundancy is one such an approach by which three ECUs perform exactly the same task. A voter then compares results and, if at least two of them deliver the same result, the system is considered to be operational. What is the availability of the resulting system? Explain.



Risk Characterization

5) According to the IEC 61508 norm, there are 5 different risk levels that are used to characterized safety-critical systems.

a) What other norm do you know that deals with risk characterization? What is the difference to IEC 61508?

b) What does such a classification or characterization of systems depend on? Explain your answer.

c) How are different risk level referred to in the above norm?

d) What is a risk graph used for?

e) According to the risk graph what are the necessary conditions for a system to be classified as SIL 3?