Prof. Dr. P. Liggesmeyer
Michael Roth, M. Sc.

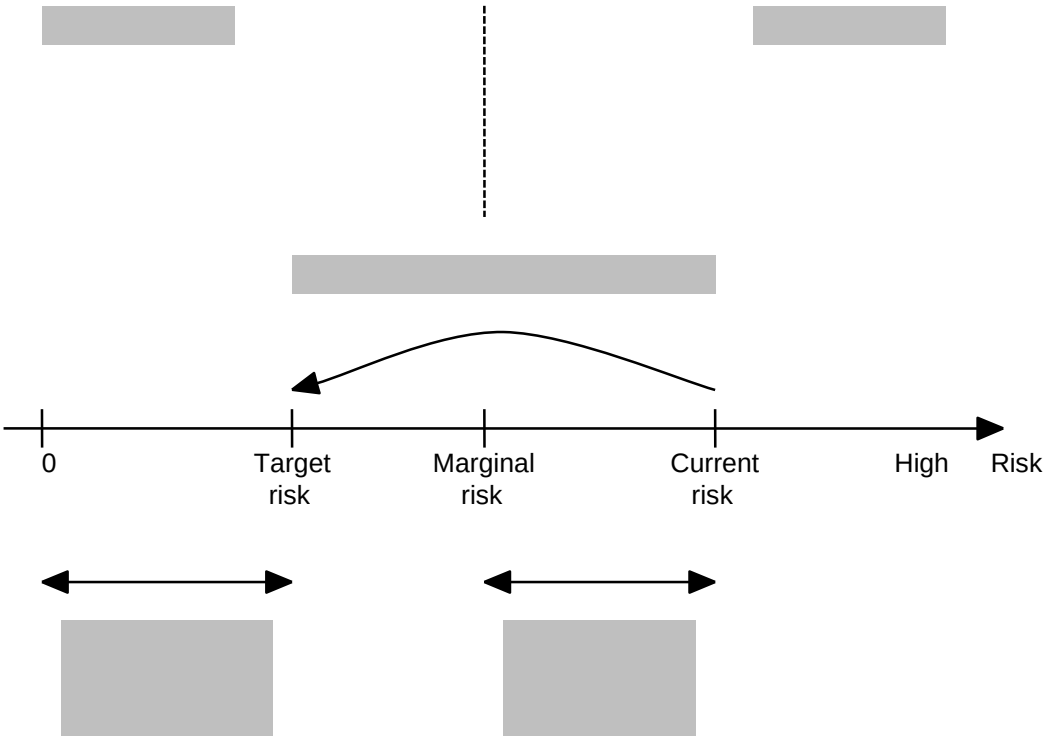
Technical University of Kaiserslautern
Dept. of Computer Sciences
AG Software Engineering: Dependability

Safety and Reliability of Embedded Systems
(WS 15/16)

Problem Set 2

Problem 1: Definition of "risk"

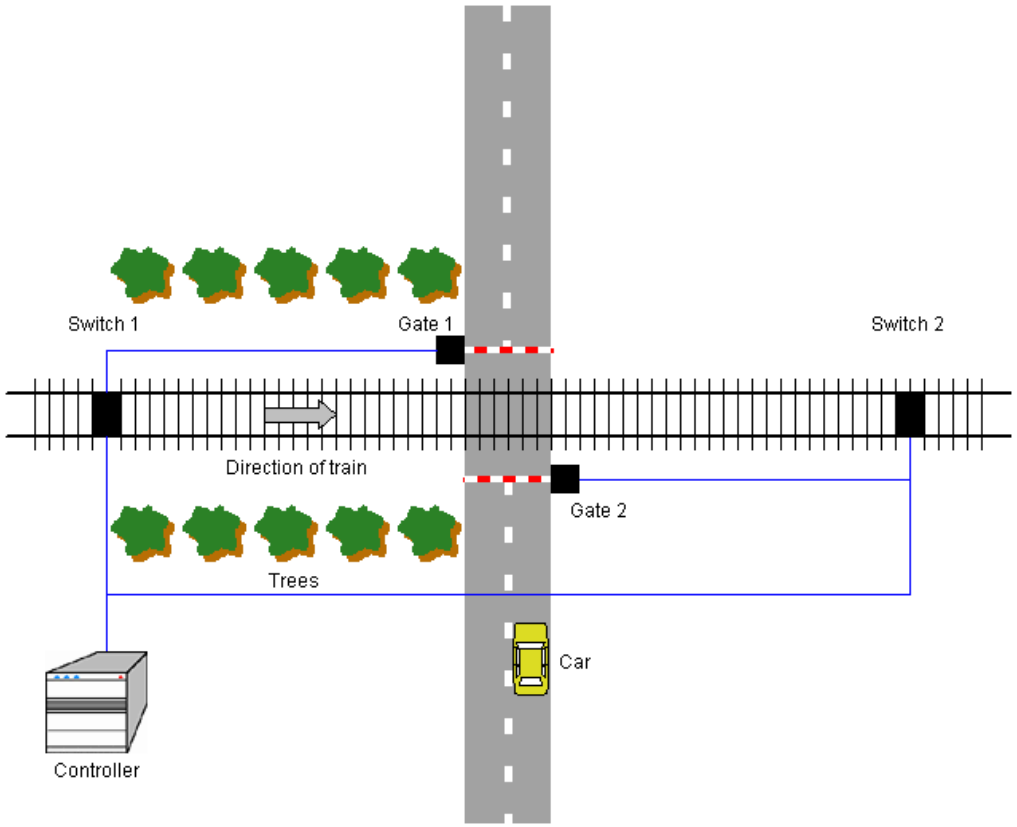
1. Complete the graphic by filling in the gray boxes with the following concepts: Safety, Danger, Residual Risk, Required Risk Reduction and Actual Risk Reduction.



2. How is risk defined mathematically? Please depict your results from 1. by using a frequency vs. severity plot.

Problem 2: Railroad crossing

Consider the following sample railroad crossing:



The crossing is equipped with a safeguarding system, which works as follows:
If a train passes switch 1, a signal is sent to the controller indicating the approaching train. The controller then sends a signal to gates 1 and 2, causing them to close. If the train finally has passed switch 2, a corresponding signal is sent to the controller, which in turn triggers both gates to reopen.

The safeguarding controller now shows a failure leading to both gates being permanently held open. The crossing is therefore in a hazardous state and an accident (train crashes in car) could happen. Usually after 12 hours, this hazard is detected by railway personnel and operation is restored to normal mode immediately. The railway personnel knows from experience that such a hazard happens on average every six months, and that in such a case, every hundredth crossing of a car results in an accident killing all passengers within the car.

Now consider a driver of a car using the railroad crossing approx. 300 times per year. It takes him about 5 seconds to cross the railway. Since there are trees planted alongside the railway, the driver cannot see if a train is approaching. Therefore, he is relying entirely upon the correct operation of the gates.

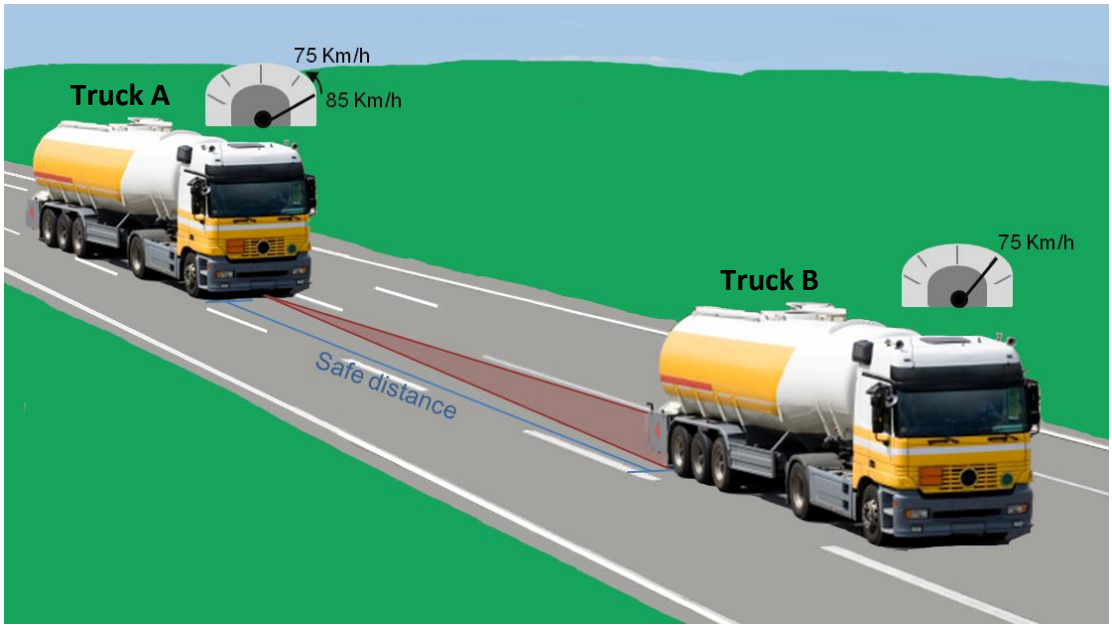
1. Calculate the Individual Risk of Fatality (IRF) for the driver of the car.
2. Is the “minimal endogenous mortality” criterion (MEM) satisfied?
3. Calculate the availability a_c of the safeguarding controller.

Problem 3: Adaptive Cruise Control System

1. You work for the quality assurance department of a car company and your manager asks you to determine the Safety Integrity Level (SIL) of the Adaptive Cruise Control (ACC) system, which will be launched in the newest car models. In order to do so, you will use the Risk Graph Method (RGM) that is introduced in Chapter 3 - "Risk Acceptance Methods". In the following you will find a description of the ACC system as well as the information that you require in order to apply RGM.

   ACC System

   The ACC system is an extension made to the Cruise Control (CC) system. Besides allowing a driver to set a constant cruise speed and to continue driving without pressing the accelerator, the ACC automatically regulates the set speed according to the current traffic situation. In case a successor vehicle is slower, the ACC reduces the speed accordingly so that a safe distance between the two vehicles is kept.



   In the figure above we can observe that Truck B is going at a speed of 75 Km/h and Truck A is going at a speed of 85 Km/h. The ACC system installed in Truck A will reduce the speed accordingly (75 Km/h) so that a safe distance to Truck B is kept. Whenever there are no vehicles ahead Truck A, the system will return the speed to the initial value set by the driver (85 km/h). The ACC is composed out of the following modules:

   - Control Logic Unit (CLU): decides if the vehicle should be accelerated or decelerated depending on: i) how fast a vehicle in front is and ii) how big the distance to a vehicle in front is. An increase or decrease of the vehicle's speed is done by the Accelerator and Brake actuators respectively, via the Acceleration and Brake Interfaces. Additionally, the CLU process driver's commands from the cockpit to set and reduce or increase the speed if necessary.
   - Brake and Acceleration Interfaces (BI, AI): act as a bridge between the CLU and the Brake and Accelerator actuators respectively.

Risk Graph Method (RGM)

This method allows a system analyst to estimate the SIL level of a system or component in a qualitative or quantitative basis. The basic assumption is that if a system fails, the nature of the resulting hazardous event (if any) is described by using four parameters (DIN EN 61508: 2010):

- Consequence of the hazardous event (C)
- Frequency of and exposure time in the hazardous zone (F)
- Possibility of failing to avoid the hazardous event (P)
- Probability of the unwanted occurrence (W)

Each parameter has a range of predetermined values, which in combination result in a required risk reduction. Based on this required risk reduction a SIL level is assigned to a hazard. All possible combinations of C, F, P and W values are depicted in a risk graph. For completing this task you will use the risk graph example provided in Chapter 3, in which you will also find more detailed information about the parameters and their values.

Hazards of the ACC

For simplicity reasons you will consider two hazards, based on the following accident scenario:

Accident	Hazards
Crash with a vehicle in front	Acceleration is too high Deceleration is too low

SIL Ranking

1. Please give a C,F,P,W value for the hazards based on the values described in Chapter 3 and on the following assumptions (notice that they are not based on real data):

    - If an accident occurs due to these hazards, at least 2 people are killed and at most 10 people are killed.
    - There is a high possibility to avoid these hazards by deactivating the ACC system and giving the full control of the vehicle to the driver.
    - It is known that each hazard might occur once in 10 years.
    - According to a safety analysis, the likelihood that the ACC system is in a hazardous state is 0,02%.
    - The ACC vehicle's passengers (including driver) sit inside the vehicle two hours per day in average.

2. Assign a SIL level for the ACC system by ranking the Hazards using the risk graph example provided in chapter 3. What is the necessary risk reduction to be applied?