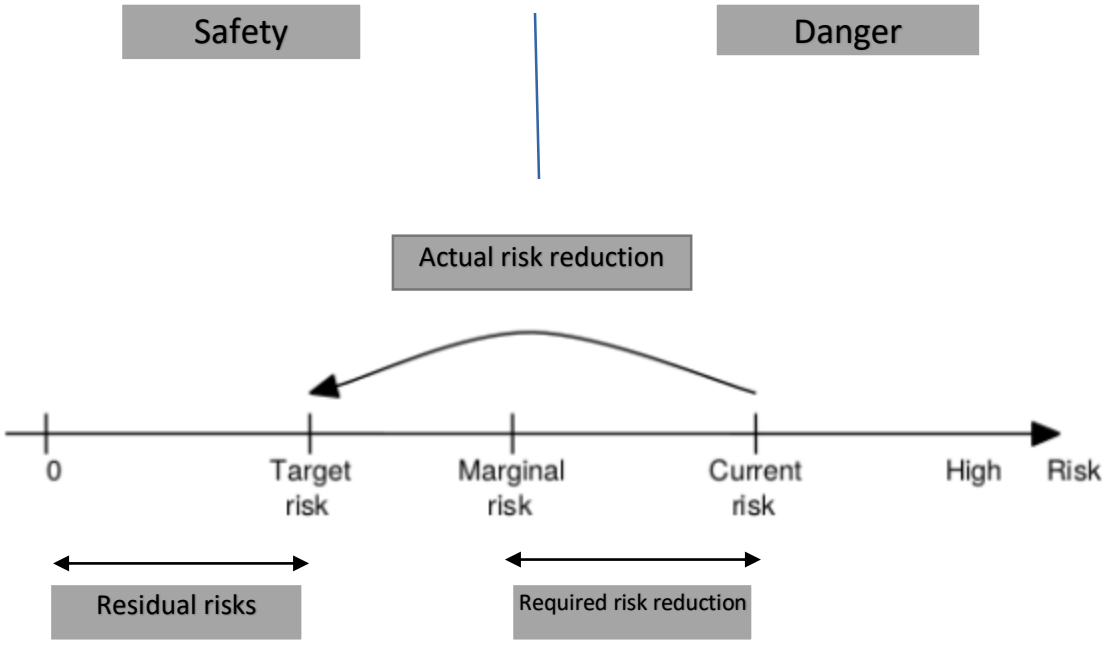
Safety and Reliability of Embedded Systems- SRES (WS 19/20)
Problem Set 2

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.*

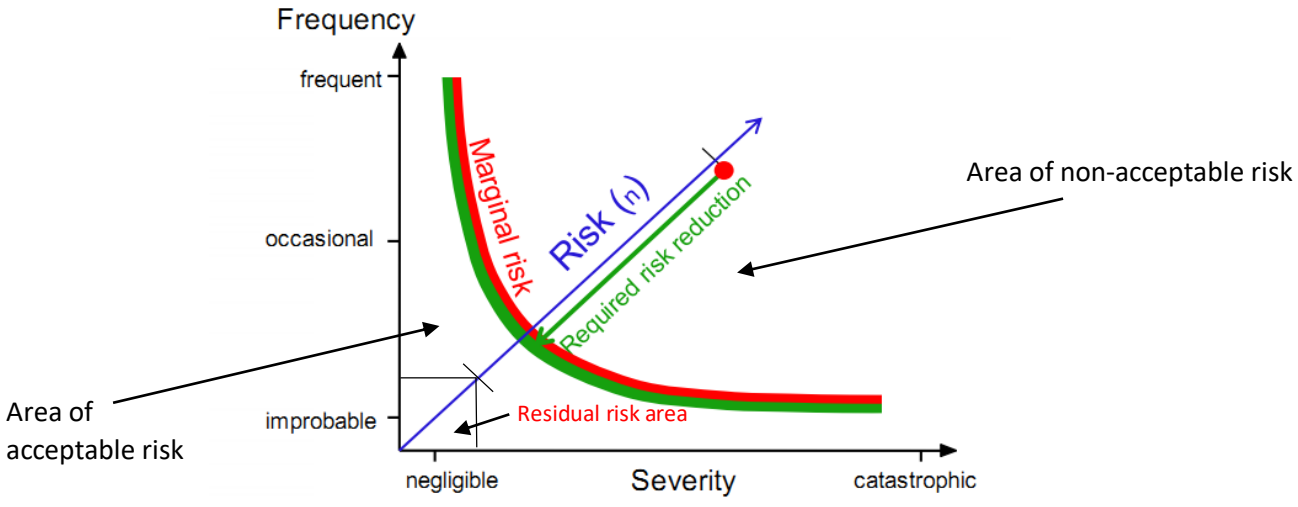
-



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

-

Definition of risk: R = H * S
H: Expected frequency of the occurrence of an event that leads to a particular harm.
S: Expected severity of the harm



Problem 2: Railroad crossing

summary: MTTR = 12 hours
MTBF = 6 months

Every 100 [th] crossing accident killing all passengers

Driver: 300 railroads crossings per year
5 seconds per crossing

1. *calculate the individual risk of fatality for the driver of the car.*

-

NP = $\frac{300}{y}$ = $\frac{300}{8760h}$ = $\frac{5}{146h}$ = $3.42 \times 10^{-2} h^{-1}$

HR = $\frac{2}{y}$ = $\frac{2}{8760h}$ = $\frac{1}{4380h}$ = $2.28 \times 10^{-4} h^{-1}$

D = 12h

E = 5 sec = $\frac{5}{3600h}$ = 0.001388 << D = 0

C = $\frac{1}{100} = 0.01$

$$IRF_i = \sum_{hazard_j} NP_i \cdot \left[HR_j \cdot (D_j + E_{ij}) \cdot \sum_{accidents_k} A_{jk} \cdot F_{jk} \right]$$

F = 1_death

So, Individual Risk of Fatality (IRF) = NP. [HR(D+E).C.F]

$= (3.42 \times 10^{-2} h^{-1}) * (2.28 \times 10^{-4} h^{-1}) * 12h * 0.01$ death

= $9.35 * 10^{-7}$ deaths/h

= $8.2 * 10^{-3}$ deaths/year

2. *is the "Minimal Endogenous Mortality" criterion (MEM) satisfied?*

-

"minimal endogenous mortality" MEM considers 10-5 deaths per person and year to be the upper limit of the (additional) mortality caused by technical systems:

$\left(10^{-5} \frac{deaths}{person.year}\right) * 1\ person = \frac{10^{-5}\ deaths}{8760h} = 1.142 * 10^{-9} \frac{death}{h}$

IRF = $9.35 * 10^{-7} \frac{death}{h} > 1.142 * 10^{-9} \frac{death}{h}$

So, the MEM criterion is not fulfilled.

3. calculate also the availability a_c of the safe guarding controller.

-

$a_c = \frac{MTBF}{MTBF+MTTR} = \frac{4380}{4380+12} = 0.99727$

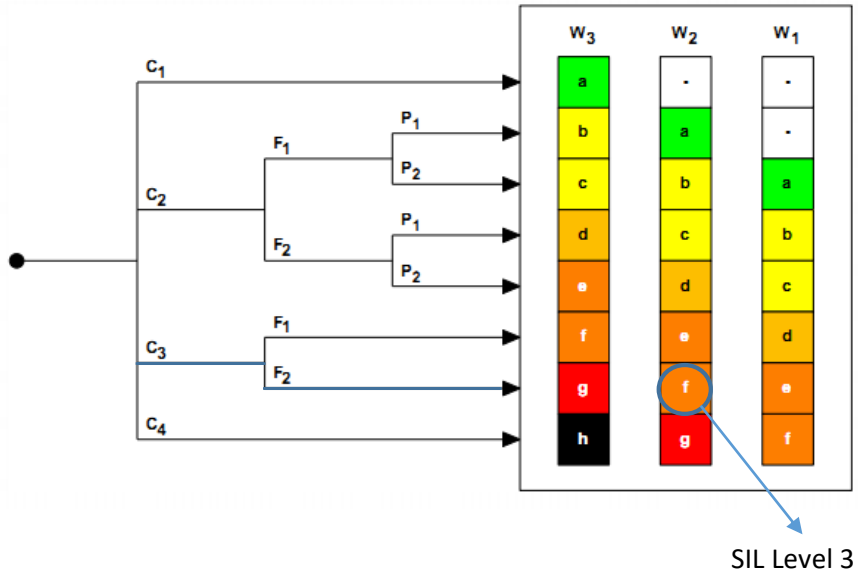
Problem 3: Adaptive Cruise Control System

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):
   - Acceleration is too high
   - Deceleration is too high

*** Reference: Slide 30, Chapter 3

Consequence **C = C_3**	If an accident occurs due to these hazards, at least 2 people are killed and at most 10 people are killed. **(C_3: Death of several people)**
Frequency of and exposure time in the hazardous zone **F = F_2**	The ACC vehicle's passengers (including driver) sit inside the vehicle two hours per day in average. **(F_2:Frequent to permanent)**
Possibility of failing to avoid the hazardous event **P = P_1**	There is a high possibility to avoid these hazards by the deactivating the ACC system and giving the full control of the vehicle to the driver. **(P_1: Possible under certain conditions)**
Probability of the unwanted occurrence **W = W_2**	• It is known that each hazard might occur once in 10 years. (few unwanted occurrences -> 1/87600 $\approx 1.141\times 10^{-5}$ • According to a safety analysis, the likelihood that the ACC system is in a hazardous state is 0.02% **(Slight probability)**

2. *Assign a SIL level for the ACC system by ranking the Hazards using the risk graph example provided in chapter* -



Necessary minimal risk reduction	Safety integrity level
-	No safety requirements
a	No special safety requirements
b, c	1
d	2
e, f	3
g	4
h	An E/E/PE SRS* is not sufficient

* Electrical/Electronic/Programmable Electronic safety-related system

SIL Level 3

*** Reference: Slide 29, Chapter 3

3. What is the necessary risk reduction to be applied?
   -
   Minimum required risk reduction: f