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

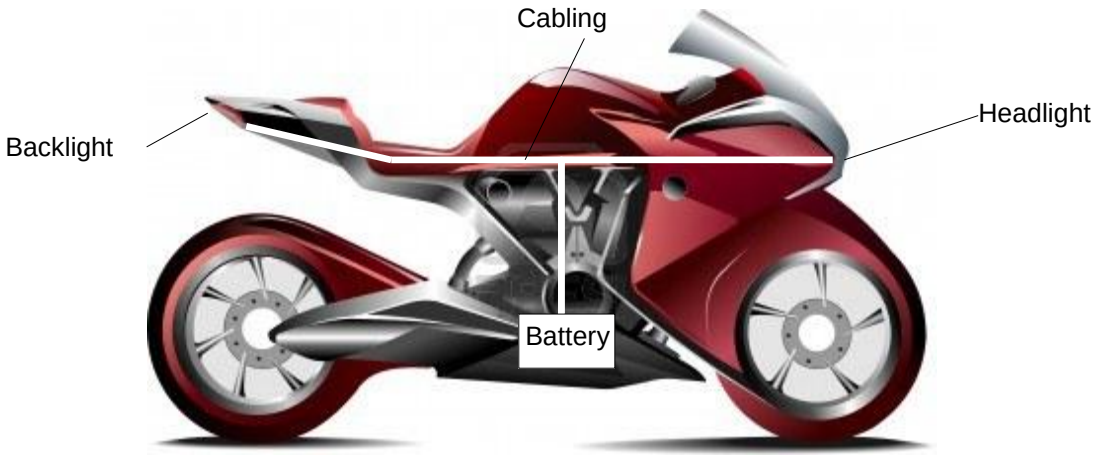
Technical University of Kaiserslautern
Dept. of Computer Sciences
AG Software Engineering: Dependability

Safety and Reliability of Embedded Systems
(WS 12/13)

Problem Set 4

Problem 2: FMECA

You work for the quality assurance department of a motorbike manufacturer company and your manager asks you to do a "Failure Modes, Effects, and Criticality Analysis" (FMECA) for the complete light system of the newest product:



The headlight and backlight are both composed of the following parts:
- housing
- bulb
- socket (for bulb)
- reflector
- frame mount

The cabling consists of these parts:
- isolation
- wire
- cable mount

The battery is treated as an encapsulated component and is not decomposed any further.

From your experience in the field of electrical lighting systems for motorbikes, you know that you have to consider the following aspects during the analysis:
- humidity, corrosion
- mechanical damage, cracks
- loose-fitting parts, screws not tightened
- wrong/defective bulbs

- broken wires, short circuit
- high contact resistance, no electrical contact
- uncharged/half-charged/broken batteries

1. With this knowledge please do a FMECA for the headlight/backlight of the motorbike by using the given template (see Annex 1). Do a further analysis for other components of the light system of the motorbike and assign rankings for severity of consequences (S), occurrence probability (O), and probability of non-detection (D). After this calculate the associated risk priority numbers (RPN) and find out on which failure modes you have to focus first? What are your suggestions for corrective measures?
2. The failure mode "Light works intermittently" has to be further analyzed by using Fault Tree Analysis. Please create the corresponding fault tree(s) by using the results of your FMECA.

Problem 2: K out of N system

You have to evaluate the failure of a 2 out of 3 system with the help of Fault Tree Analysis. A 2 out of 3 system consists of 3 components and for the system to be operating at least two out of these 3 components have to be operating. Please consider the following events for your analysis:

Event type	Name	Description	Probabilities
Top event	F_{sys}	2 out of 3 system fails	f_{sys}
Intermediate event	F_{12}, F_{13}, F_{23}	Two components fail	f_{12}, f_{13}, f_{23}
Basic event	F_1, F_2, F_3	A single component fails	f_1, f_2, f_3

The probability of failure of each single component is assumed to be $f_c = 0.03$

a) Please draw the corresponding fault tree using the above event names.
b) Try to calculate the probability of failure of the system f_{sys} by applying standard gate formulas known from lecture in a bottom-up fashion.
c) Now determine the minimal cut sets and calculate an approximation for f_{sys}.
d) Finally, draw a binary decision tree for f_{sys} using the variable order $F_1 \rightarrow F_2 \rightarrow F_3$. Convert the tree into a reduced ordered binary decision diagram (ROBDD). Annotate the diagram with probabilities and again calculate the availability f_{sys}.
e) Compare the three results.

Annex 1

Ref. no.	Component	Failure mode	Effect of failure	Failure cause	S	O	D	RPN	Corrective measures
1	Bulb	Light works intermittently	*No light*	*Defective bulb*	*8*	*4*	*2*	…	*Test bulb before assembly*
2				*Loose-fitting bulb within socket*	*8*	*6*	*7*		*Check fitting of bulb during assembly*
3				*Broken wire*	*8*				*Measure wire resistance before assembly*
4				Short circuit	*8*				*Use cable bushing to prevent damage to isolation of cable*
5				*Uncharged battery*	⋮	⋮	⋮		
6				Broken battery					
7				Broken soldering joint(s)					
⋮	⋮								

S: severity of consequences (1 … 10)
O: occurrence probability (1 … 10)
D: probability of non-detection (1 … 10)
RPN: risk priority number (1 … 1000)
(For your guidance, please have a look at slide 6 chapter 5 of the lecture)