Design and Integration of Embedded Systems exam SOLUTION **December 16, 2020.**

Available time: 60 minutes

Maximum points: 24. Minimum points needed: 12 points

Please start solving each exercise on a separate page, writing first your name and Neptun code.

Exam topics: System Design (12 points)

1. You are starting a new small company (10-15 person) with your colleagues. You have learnt about process models and CMMI. Your colleagues turn to you for advice to create the processes of the new company:

   a. Which approach of CMMI would you choose and why? **(1 point)**

   For a starting company a **staged representation** is much better, because it gives guideline about which processes and in what level should be introduced at a given phase of the organization's development.

   b. Which CMMI level would be your first target, and why? **(2 points)**

   For a starting company **maturity level 2** should be the first target, because it has the minimum set of processes mainly focusing on the project planning, monitoring and control, which is essential for a controlled development, and to have an organized way of working. Higher maturity levels would probably give too much work to the employees.

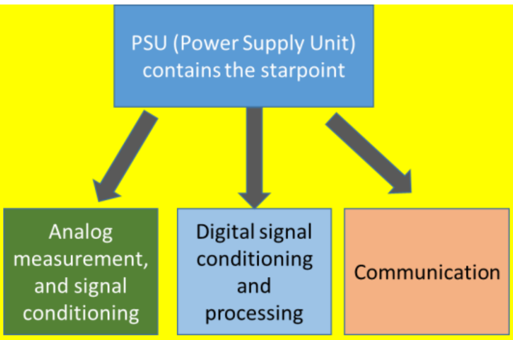
   c. In 2 years, your company start to grow and become bigger and bigger. Which minimum CMMI level could cover this growing and why? **(2 points)**

   For a bigger company a good goal is to reach **maturity level 3**, where the company get organization level control, and organization level processes. If there is not such organization level control, then things get messy for a bigger company. Each team will use their own preferred methods and tools, projects and team members cannot be re distributed easily between the teams due to these team specific methods. At this level the fluctuations of employees also become a normal thing. Companies with more than 50 people usually have an employee migration rate of 5-10% pro year, therefore the training of these new employees should be organized.

2. You have to design an embedded device with the following functionality: relatively precise analog measurement functions using a close range analog sensor (< 1m), signal conditioning and data processing of the analog measurements, communication of the results to a remote data concentrator using a wired communication like CAN bus (distance > 100m). The device will be used outdoor, but in a relatively protected environment.

   a. What type of Power supply architecture would you choose if you know that the device need to be relatively cheap? Draw the architecture and reason your decision! **(2 points)**

   For this type of device usually the star point power structure is used, if the reasoning is good, the star point with separate PSU also can be accepted. The star point power structure is good because it minimalizes the common impedance based problems in a cheap way, without adding extra components.


PSU (Power Supply Unit) contains the starpoint
Analog measurement, and signal conditioning
Digital signal conditioning and processing
Communication

b. Do you need galvanic isolation in this device? If yes, where and why? **(1 point)**

We need to galvanic isolation for the communication. Signals going far from the device should be isolated due to grounding and life protecting problems.

c. Three types of enclosures are offered to you by the sales person of the company: with IP44 (low cost), IP54 (medium cost) and with IP67 (high cost) protections. Which one would you choose and why? **(1 point)**

IP 44 is a typical in-house enclosure, it is not suitable for dusty environment. IP 54 is a typical dust resistant low duty outdoor enclosure, while IP67 is a water resistant enclosure that can be used under water. For this device the IP54 should be a good choice.

3. You are a tester in an embedded system company. You have to test the following C function, which calculates the new gear level of an automatic transmission controller:

```
// returns the new gear level: -1 to +5
int8_t newGearLevel(int16_t speedOfTheCar,    // 16-bit signed value: car speed in km/h
             uint8_t acceleratorPedalState) // 8-bit unsigned value: state of the pedal in %
```

a. How many test cases should you have in order to perform *exhaustive testing* (the module has no memory, it does not use any global variable)? **(1 point)**

If the module has no memory, then the possible combinations of input values would be an exhaustive testing. Exhaustive test cases = 2^16 * 2^8 = 2^24

b. With what technique or method could you reduce the number of test cases, and what information would you need for this technique? **(1 point)**

Equivalent partitions can be used to reduce the number of test cases. Based on the specification some value ranges can be considered as irrelevant, for example car speed below -100, or car speed above 400 etc. Input relations also can be used to create equivalent partitions for gear states, for example speed between 20-50 km/h and pedal state between 20-60% would result gear state 3.

c. Suggest some test case reduction! **(1 point)**

For example, car speed below -100, or car speed above 400 is irrelevant and can be considered one cluster. Gas pedal state above 100% is also can be considered irrelevant.

Please turn the page!

Exam topics: Safety Critical Systems (12 points)

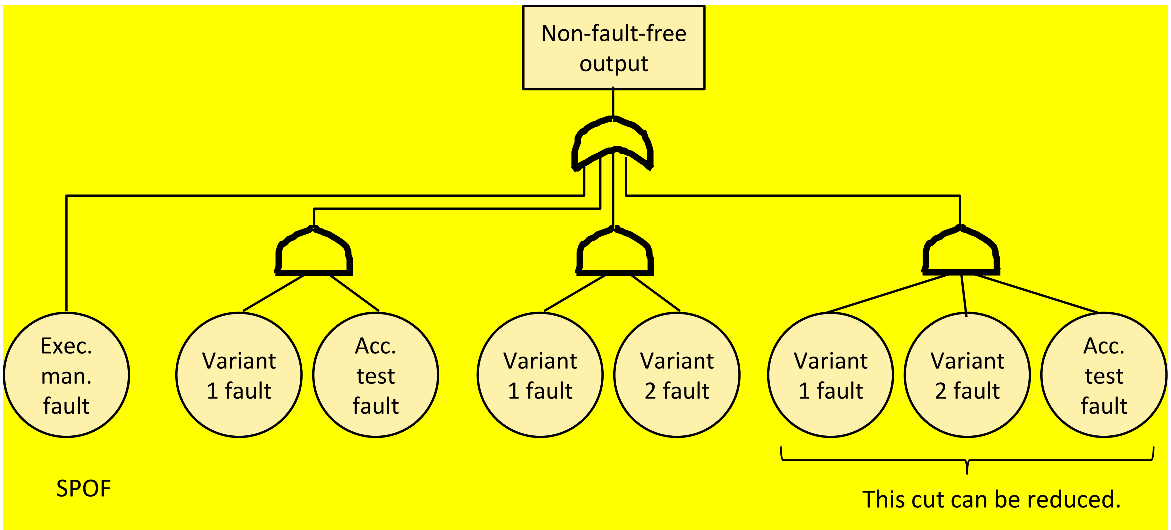
4. Consider a software system consisting of 2 *variants* (diverse components implemented to solve the same problem), an *acceptance test* module and an *execution manager* module, which implements a recovery block (RB) architectural scheme.

   a. List the *tasks* that have to be implemented by the execution manager module according to the RB scheme! **(1 point)**

   Execute the first (primary) variant, then execute the acceptance test.
   If the acceptance test reports a faulty output of the first variant, then execute the second variant and then execute the acceptance test.
   If needed in the concrete environment: save checkpoint before executing the first variant and perform recovery before executing the second variant.

   b. Draw the *fault tree* belonging to the *non-fault-free output of the system*, considering the independent faults of the components. Assume the following: if the acceptance test is faulty then it reports a faulty variant as fault-free. **(2 points)**

   The fault tree:



   c. List the *single points of failure* (or indicate, if there is no single point of failure). **(1 point)**

   Single point of failure: Fault of the execution manager.

5. The operating modes of an air conditioner can be characterized by the following propositions (labels): *Cooling, Heating, Ventilating*.

   a. Formalize the following property using the operators of the CTL temporal logic:
   For all executions, it will eventually happen that there is heating and ventilating at the same time. **(1 point)**

   $AF\ (Heating \wedge Ventilating)$

   b. Explain the meaning of the following CTL temporal logic formula, where $\wedge$ denotes Boolean conjunction and $\neg$ denotes negation:
   $EG\ (\neg\ (Ventilating \wedge Cooling))$ **(1 point)**

   There is (at least) one execution, for which globally (in all states) there is no ventilating and cooling at the same time.

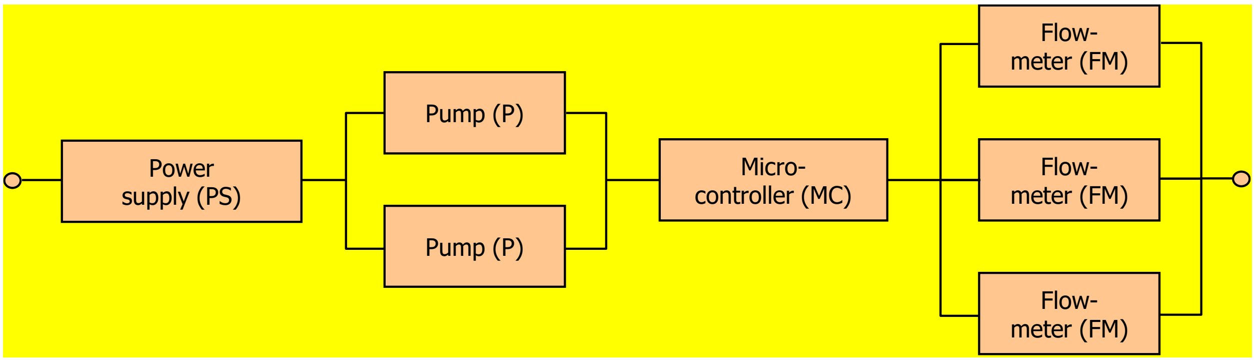
   In other words: The air conditioner can be operated in such a way that there is no ventilating and cooling at the same time.

6. A water transfer equipment consists of the following components: a *power supply*, two *pumps* (any of the pumps is sufficient to provide the service) that are controlled by a single *microcontroller*, and three redundant *flowmeters* that provide inputs to the microcontroller (any of the flowmeters can perform the flow measurement). If a flowmeter fails, then it does not provide any output. The microcontroller does not give any control in case of its fault or missing input. A faulty power supply does not provide output voltage. The characteristics of these components are as follows:

	Power supply	Pump	Microcontroller	Flowmeter
MTTF (hours)	25 000	20 000	30 000	15 000
MTTR (hours)	2	2	6	2

a. Construct the *reliability block diagram* of the equipment! **(3 points)**

The reliability block diagram:



b. Give the *formula* that can be used to compute the asymptotic *availability of a component* if its MTTF and MTTR characteristics are known. **(1 point)**

A = MTTF / (MTTF+MTTR)

c. Give the *formula* that can be used to compute the asymptotic *availability of this equipment* (in case of regular repairs of the failed components) using the asymptotic availabilities of the components! It is enough to give the formula, the result of computation shall not be provided. **(2 points)**

Let's denote the asymptotic availabilities of the components as A_{PS} (power supply), A_{P} (pump), A_{MC} (microcontroller) and A_{FM} (flowmeter).

The availability of the equipment:

$$A = A_{PS} * (1-(1-A_{P})^{2}) * A_{MC} * (1-(1-A_{FM})^{3})$$