Examination, 7.5 credits, DVA437 (DVA321) – Safety critical systems engineering

Date: 2018-06-04, 8:10–12:30

Responsible teacher: Barbara Gallina 021-101631(available to answer questions from 9:30 AM).

This is a "closed book" exam, that is, no material other than pen/pencil allowed.

Max points: 40
Approved: Minimum 20 points

Grade 5: 34 – 40 p	**Grade A:** 36 – 40 p
Grade 4: 27 – 33.9 p	**Grade B:** 32 – 35.9 p
Grade 3: 20 – 26.9 p	**Grade C:** 28 – 31.9 p
	Grade D: 24 – 27.9 p
	Grade E: 20 – 23.9 p

Write on one side of the sheet only.

Assumptions must be made when there is not enough information provided to solve an assignment, and all assumptions must be specified and explained in order to achieve full points.

Good luck!

1. Multiple choice questions (5p)

Only mark one answer per question (A, B, or C). A correct answer will give you **+1** points, and an incorrect answer will give you **-1** points.

	A	B	C
ALARP A. requires a cost-effectiveness demonstration. B. does not require a cost-effectiveness demonstration. C. ALARP is equivalent to GAMAB.			
Architectural specifications are evidence, which can be classified as: A. immediate evidence. B. direct evidence. C. indirect evidence.			
SACM is a metamodel that embraces: A. GSN only. B. CAE only. C. GSN and CAE.			
DALs are: A. Other. B. Measure of confidence used in the medical domain. C. Measure of confidence used in the avionic domain.			
The term “Bow tie” is used to represent: A. Software accident rate curve. B. Hardware accident rate curve. C. Other.			

2. Argumentation (4p)

In the context of DVA437, argumentation notations were discussed.
Which essential elements characterize them? Choose a notation and draw them (1p)

Answer:

Explain their semantics (3p).

Answer:

3. Pacemaker –Marie Mo experience (5p)

"A month before turning 34, I received an unexpected birthday gift: a cloud-connected pacemaker. It sits in a tiny pocket in the left side of my chest, just above my heart. Silently and diligently, the device emits electrical pulses to make sure my heart rate never again plummets below 25 beats per minute. The idea of a battery-equipped, internet-connected device living forever inside my chest both terrifies and fascinates me."
Taken from an interview with Marie Mo.

According to your understanding of the above-given information and of the available information (Marie Mo's lecture discussed in the context of DVA437), what is that may go wrong? List (at least one of) the threats that may contribute to the occurrence of an accident and elaborate on (it) them by using FMECA. (5p)

Answer:

(This page intentionally left blank. Space can be used for question 3)

4. Terminological framework related to dependability (6p)

Automated electronic monitoring systems in intensive care units (ICU) routinely collect vast amounts of real-time patient vital signs data, including blood pressure and electrocardiogram (ECG), via bedside monitors. If abnormalities in the vital signs are detected (e.g. if they fall outside the range of some pre-set thresholds), the monitoring system triggers the alarm and notifies the nurses or physicians in charge. However, the ICU monitoring systems often have a high level of sensitivity in detecting patients' abnormal status. While it is important to not miss any important alarms, the sensitivity leads to a high false alarm rate, resulting in a common phenomenon known as *alarm fatigue*. Alarm fatigue for medical staff may lead to longer response time or missing of important alarms.

a) Make use of the terminological framework related to dependability and to the etiology of accidents to describe what according to you might happen (highlight threats and any eventual causation relationship). (3p)

Answer:

b) Discuss potential counter-measures by showing your knowledge w.r.t. counter-measures classification. (3p)

Answer:

(This page intentionally left blank. Space can be used for question 4)

5. Normal accidents (5p)

Charles Perrow discussed about “Normal accidents”.
What is a normal accident? (2p)
In which circumstances normal accidents occur? (3p)

Answer:

6 ISO 26262 (5p)

Describe the ISO 26262-compliant reference life-cycle model for SEooC (5p).

7. Safety case (10p)

According to FDA (https://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/GeneralHospitalDevicesandSupplies/InfusionPumps/), "an infusion pump is a medical device that delivers fluids, such as nutrients and medications, into a patient's body in controlled amounts.

Infusion pumps offer significant advantages over manual administration of fluids, including the ability to deliver fluids in very small volumes, and the ability to deliver fluids at precisely programmed rates or automated intervals.

In general, an infusion pump is operated by a trained user, who programs the rate and duration of fluid delivery through a built-in software interface. Many infusion pumps are equipped with safety features, such as alarms or other operator alerts that are intended to activate in the event of a problem. For example, some pumps are designed to alert users when air or another blockage is detected in the tubing that delivers fluid to the patient. Some newer infusion pumps, often called smart pumps, are designed to alert the user when there is a risk of an adverse drug interaction, or when the user sets the pump's parameters outside of specified safety limits.".

Argue about (or against) increased safety thanks to the usage of an infusion pump?
Use GSN to develop your argumentation. Use well-known GSN patterns, if appropriate.
Remark: your goal structure(s) can be preliminary.

Answer:

(This page intentionally left blank. Space can be used for question 7.)