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

Date: 2019-08-15, 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 4: 27 – 33.9 p
Grade 3: 20 – 26.9 p

Grade A: 36 – 40 p
Grade B: 32 – 35.9 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!

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

Date: 2019-08-15, 8:10–12:30

---

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
Imagine you are browsing a site and you are interrupted by an ad suggesting you to enter some confidential data to get a $10,000 gift card. What is more likely: A. You are selected randomly among the active users and you will get the gift card, if you follow the suggestion. B. your PC/laptop is infected and you have safety threat. C. none of the above.			
A requirements specification can be classified as: (A.) immediate evidence. B. direct evidence. C. indirect evidence.	✓		
The IEC 61508 represents a standardization framework applicable to: A. the rail domain. (B.) any domain in absence of a sector-specific one. C. the medical domain.		✓	
The incomplete identification of potential hazards is related to: A. epistemic doubt. B. logical doubt. (C.) both.			✓
The RAMS process stands for: (A.) none of them. B. Reliability, Accuracy, Maintainability, Safety. C. Reliability, Accuracy, Maintainability, Security.	✓		

2. Argumentation (8p)

a) How would you label this argument?
"Global warming doesn't exist because the earth is not warmer"
Is it fallacious? Motivate your answer. (2p)
Answer:

yes it is. Because global warming exists even tho we can't feel it at the moment. But if we compare temperatures onudy we will see that the temperature tend to go higher.

b) How would you label this argument?

if P, then Q
Q exists
therefore P exists

Is it fallacious? Motivate your answer. (2p)

Answer:

yes it is, because based on these lines we understand that when Q exists or it's true consequentially P must exists or be true as well, but this is not always true.
I can provide an example below which can prove that.

example: if the car has no spark plugs, then it won't start up
let's supose that "it won't start up" exists
then spark plugs are not the only reason that can cause this problem there are other reasons as well.
so this is not true.

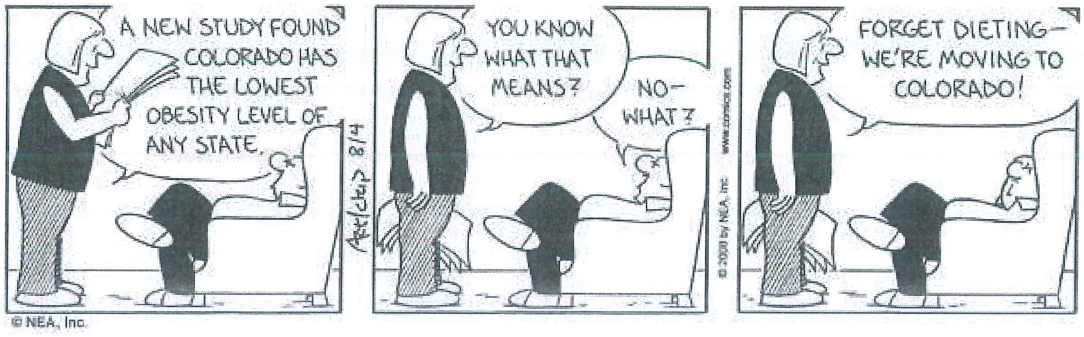


Figure 1

c) How would you label the argument represented in Figure 1?

Is it fallacious? Motivate your answer. (2p)

Answer:

yes it is, because if they move to Colorado they are not going to be less obese when they actually are. Because this are just statistics for people who actually live there.
So, that is not going to affect them at any point.

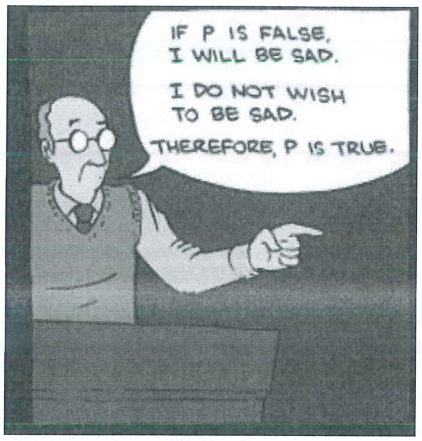


Figure 2

d) Consider Figure 2, is there any similarity between the argument formulated in it and the arguments which were proposed in question a), b), c)? (2p)

Answer:

3. Accident investigation-pacemaker (12p)

Consider the following piece of information:

"The first person in Britain to receive what was heralded as a revolutionary pacemaker has told of her nightmare after it stopped working and surgeons were unable to extract the implant from her heart.

Maureen McCleave, 82, from Chingford in Essex, said she felt "so lucky" when in 2014 she was offered the Nanostim device, which is a 10th the size of a traditional model and the first of its kind to be approved."

Figure 3 provides a representation of the device and of the process used to deploy it.

"However, within three years McCleave began suffering from dizziness, palpitations and exhaustion.

Doctors discovered the pacemaker's battery, which was meant to last 10 years, had died. McCleave was one of dozens of patients placed at risk due to this technical flaw, which prompted an official safety alert.

The cases raise questions about whether the device was sufficiently tested before being approved and whether patients who were fitted with the pacemaker were fully aware of the risks.

She was given the Nanostim weeks after it was awarded its CE (Conformité Européenne) safety mark by Britain's leading approval body, the British Standards Institution.

McCleave received a letter about the battery issue but said she assumed she was unaffected. But in January 2017 she began to suffer dizziness, palpitations and exhaustion and felt "something, somewhere was wrong".

When she attended hospital, doctors discovered the battery on her pacemaker had drained prematurely and she was sent for urgent revision surgery. Although Nanostim was marketed as retrievable, McCleave was advised it could not be taken out and a conventional pacemaker was added in alongside it.

In November 2017, Abbott, which had acquired St Jude, issued a further safety notice warning of a problem with the docking button that was designed to allow doctors to extract the device. This included three reports of the button detaching and in one case migrating into an artery.

Francis Murgatroyd, the director of cardiac electrophysiology at King's College hospital in London, said he feared St Jude was "in a rush" to bring Nanostim to market ahead of a competing leadless pacemaker being developed by a rival medical device company, Medtronic. "My impression was that the company was very, very pushy."

In the US, the Food and Drug Administration has not approved Nanostim for use on patients, despite the device having been initially developed in the US."

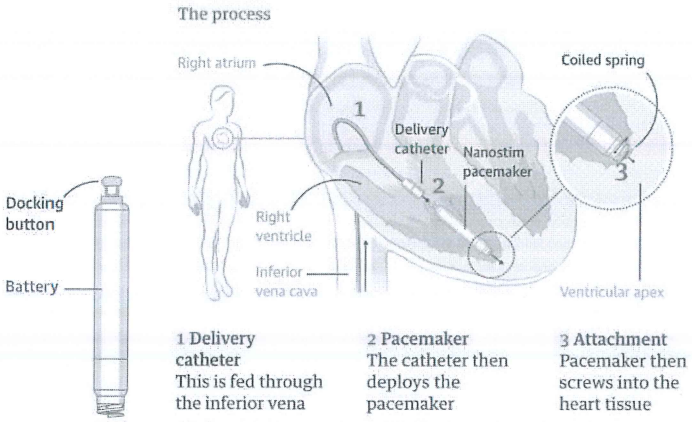


Figure 3 Pacemaker and pacemaker's deployment

Taken from: https://www.theguardian.com/society/2018/nov/25/faulty-pacemaker-nanostim-raises-concerns-medical-device-testing

List at least four of the threats (two related to an organization-component, and two related to a technical-component) that may contribute to the occurrence of accidents and elaborate on them by using the combination of Reason's model & Randell's model. (12p)

Answer -organization component-1:

1- Development fault.
nanostim pacemaker was not developed and tested properly.

Answer -organization component-2:

2- malicious fault.
this mistake can lead to fatal consequences.

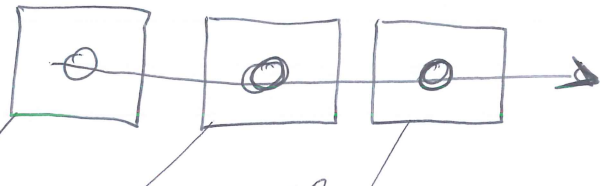
Answer -technical component-1:

1- Hardware faults
the fault mitigated from the device

Answer -technical component-2:

2- internal faults

the fault come whithin the device which is located inside the heart.



fault : there was a problem with nanostim.
error : this problem was non detected during testing phase
failure : the device was deplaed with the problem remaining in it.

fault : The device was attached to human body
error : the problem was not detected during operational mode
failure : the human body was in serious critical condition.

fault : battery starts to drain.
error : the effect of the battery started to mitigate through the body
failure : the human body was not in proper conditions which is a ~~potentional~~ potentional ~~sor~~ source of harm.

4. Terminological framework related to dependability (6p)

In Kitakyushu City on the island of Kyushu, at about 9:40 in the morning, a blackout occurred on the JR Kagoshima Line between Moji Station and Space World Station as well as the Nippo Line running between Kokura and Jono Stations. In total, 26 train routes were affected running in all directions and approximately 12,000 people were affected by delays that lasted about an hour.

Railway workers traced the source of the blackout to a piece of equipment called a disconnector switch. This is a switch that diverts the electricity from a part of a system so that repairs or maintenance can be safely done on it.
Disconnector switches are only used during those times, and because their purpose is safety, they must be guarded from people and the elements. In this case, the switch was housed in a box with all its openings sealed with glue to prevent insects or small animals from wandering inside.

However, when rail crews opened a disconnector switch on the Kagoshima Line between Moji and Kokura Stations, they found the body of a slug that appeared to have been electrocuted. More impressive than the JR workers' ability to determine the slug's cause of death is the fact that it got in the highly-sealed container to begin with.
Prof. Ryota Matsuo of Fukuoka Women's University confirmed to media that slugs are capable of compressing their bodies to fit into surprisingly narrow crevices. In this case it seems the slug managed to find a tiny unsealed gap in the disconnector switch casing. Once inside, it must have touched a cable and short-circuited the entire section of railway.
Text adapted from: https://soranews24.com/2019/06/23/lone-slug-disables-26-trains-in-kyushu-for-one-hour/

a) Make use of the terminological framework related to dependability and to the etiology of accidents to describe the scenario, which can be extracted from the piece of news given above. Highlight threats and any eventual causation relationship. (3p)

Answer:

Availability => correct service was not available for further usage.

Reliability => correct service of trains was not implemented.

Safety => safety case was provided properly.

threats => operational faults, internal faults, human made faults, transient faults, accidental faults.

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

Answer:

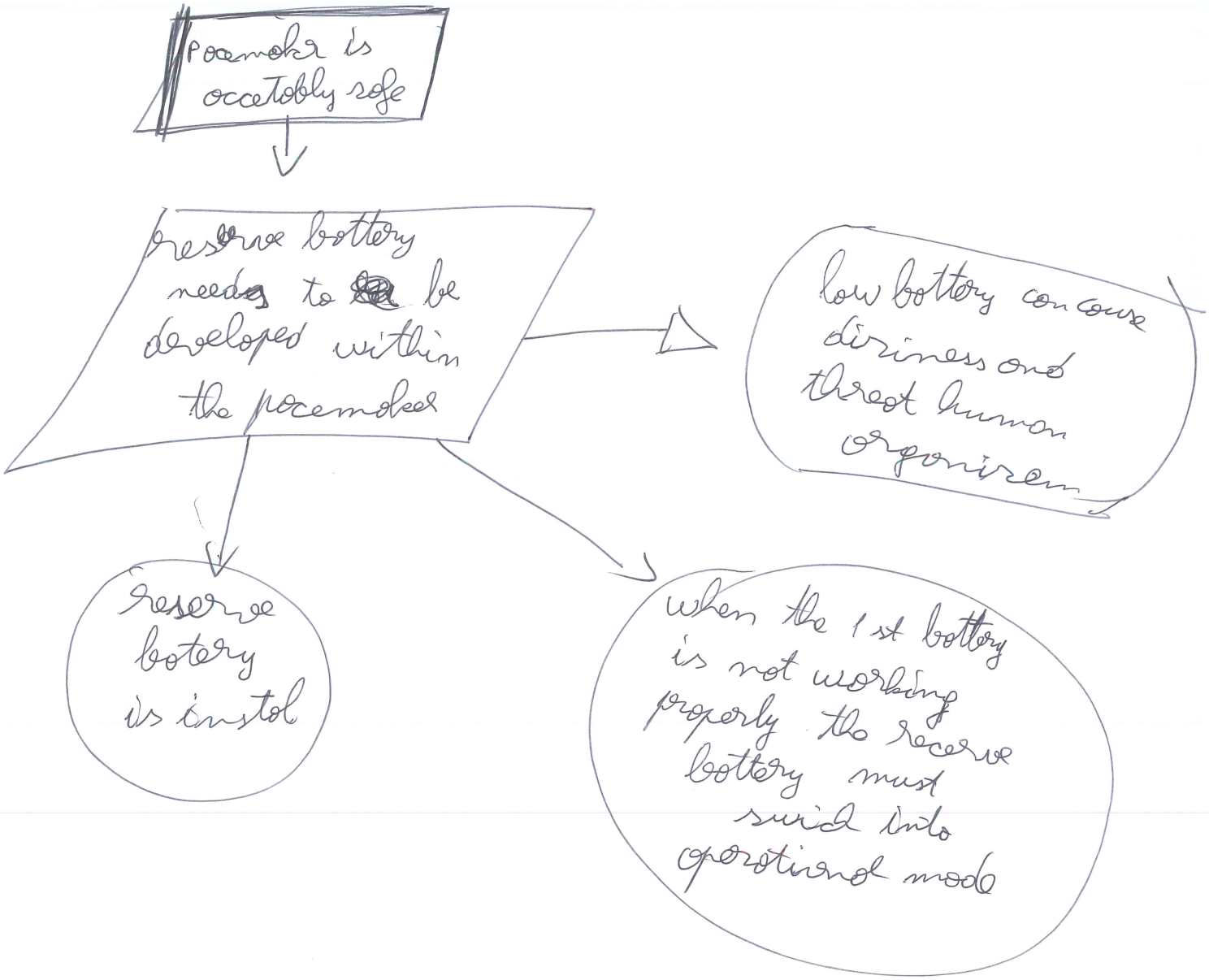
- Sanity check => uses known semotic properties of data to detect error.
- reversal check => uses the output of a module to compute the corresponding input.
- watchdog timer => detect whether a task overrun it's scheduled processing time.
- intrusion detection => monitors network/system activities for malicious activities or policy violations and reports to a management station.
- control + monitor => 2 ~~components~~ combinations C + M, M implements a ~~kind~~ simple ~~loop~~ logic to provide a degraded service compared to complex service provided by C.
- N - version Programming => N VP uses 2 or more N versions of independetly implemented software components to provide some service.

- Recovery Blocks => Sequential execution of multiple versions of a component.

5. Safety case (9p)

Based on your findings (achieved by answering question 3), provide a safety case to show that a patient cannot be safe with Nanostim pacemaker. To represent your safety case, use GSN. Use well-known GSN patterns, if appropriate.
Remark: your goal structure can be a preliminary one.

Answer:



(This page intentionally left blank. Space can be used for question 5.)