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

Date: 2019-01-17, 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!

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

ASIL:
A. QM is a safety related ASIL.
B. QM represents the highest level of quality management.
C. QM denotes no requirement to comply with ISO 26262.

Verification results are evidence, which can be classified as:
A. immediate evidence.
B. direct evidence.
C. indirect evidence.

Mary Moe on twitter states: "Yes, my pacemaker went into failsafe mode due to bitflips in the memory caused by cosmic radiation, while I was flying." Is *cosmic radiation* a:
A. External Error.
B. Internal Error.
C. Other.

The dependability attribute threatened in Figure 1 is:

Figure 1

A. Safety.
B. Reliability.
C. Confidentiality.

The "Bow tie" representation may indicate:
A. an HAZOP-like analysis.
B. FMEA.
C. FTA.

2. Argumentation (6p)

In the context of argumentation, define the notion of "fallacy" (1p).

Answer:

and enumerate at least two types (1p).

Answer:

Exemplify these two types by providing examples by using GSN (4p).

Answer:

(This page intentionally left blank. Space can be used for question 2)

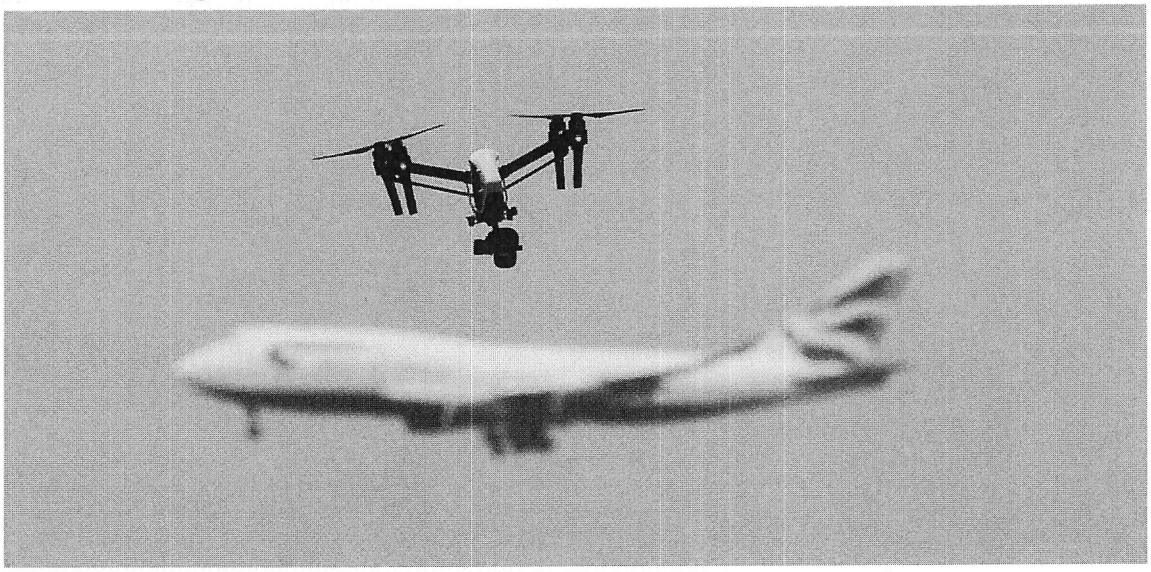
3. Accident investigation – Wireless Pressure-Sensing Eye Implant (5p)

The implantable sensor is designed for monitoring the eyes of patients with glaucoma, a disease that causes gradual loss of vision, usually as a result of excessively high pressure inside the eye. The implantable pressure sensor can reside in the human eye for years at a time while wirelessly sending data about the eye's health to the patient or medical professionals. It consists of a pressure sensor, control circuitry, and an antenna. The implant has no battery, making it small and long lasting. During a reading, radio waves from a handheld scanner are received by the antenna and generate a small voltage that temporarily powers up the device, which then takes a pressure reading and sends the signal back to the reader using the same antenna. List (at least one of) the threats that could 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)



Drones flying close to Gatwick have grounded flights (PA/file pic)

"Tens of thousands of passengers have been disrupted by drones flying over one of the UK's busiest airports.

Gatwick's runway has been shut since Wednesday night, as devices have been repeatedly flying over the airfield.
The shutdown started just after 21:00 on Wednesday, when two drones were spotted flying "over the perimeter fence and into where the runway operates from"."
[taken from BBC https://www.bbc.com/news/uk-england-sussex-46623754]

a) Assume that the piece of news is correct and make use of the terminological framework related to dependability and to the etiology of accidents to describe:
    a. what happened (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. ISO 26262 (3p)

Explain what Figure 2 represents in the context of ISO 26262 (3p).

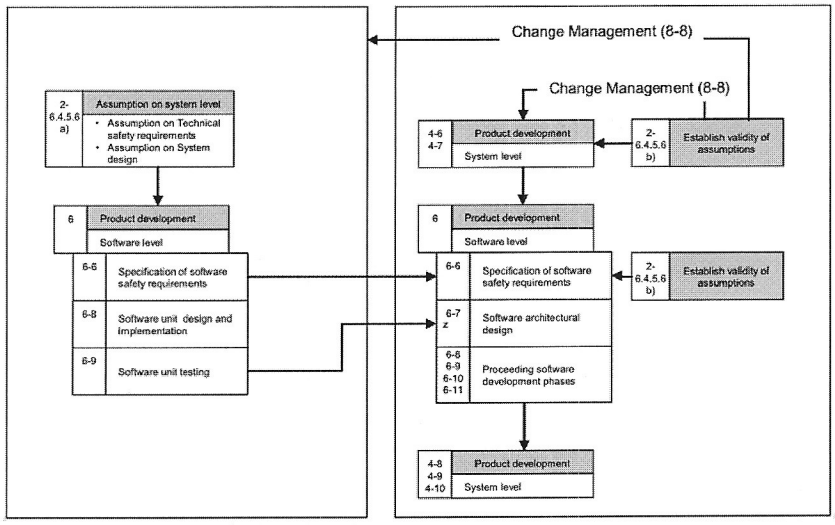


Figure 2 ISO 26262-related-figure.

Answer:

6 ISO 26262 (5p)

Requirement states: "*the software architectural design shall be described with appropriate levels of abstraction by using the notations for software architectural design listed in Table 2" (reported below)*. (5p).

Table 2 — Notations for software architectural design

Methods		ASIL			
		A	B	C	D
1a	Informal notations	++	++	+	+
1b	Semi-formal notations	+	++	++	++
1c	Formal notations	+	+	+	+

Is this requirement a product or a process-related requirement? Why? (1p)

Answer:

Assume that a UML-based architectural specification has been delivered by the design-team for software-ASIL-D.

Play the role of the safety engineer and argue in CAE about/against compliance with the ISO 26262 requirement (4p).

Answer:

7. Safety case (10p)

According to EN50128, an implementer shall have the following competence.

Key competencies:
1. shall be competent in engineering appropriate to the application area
2. shall be competent in the implementation language and supporting tools
3. shall be capable of applying the specified coding standards and programming styles
4. shall understand all the constraints imposed by the hardware platform, the operating system and the interfacing systems
5. shall understand the relevant parts of EN 50128

In order to take the following responsibilities:
Responsibilities:
1. shall transform the design solutions into data/source code/other design representations
2. shall transform source code into executable code/other design representation
3. shall apply safety design principles
4. shall apply specified data preparation/coding standards
5. shall carry out analysis to verify the intermediate outcome
6. shall integrate software on the target machine
7. shall develop and maintain the implementation documents comprising the applied methods, data types, and listings
8. shall maintain traceability to and from design
9. shall maintain the generated or modified data/code under change and configuration control

Argue about (or against) your adequate competence to take the expected responsibilities in the rail context.
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.)

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