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

**Date: 2019-06-13, 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.

Imagine you are the pilot of one of the planes within the scenario depicted in Figure1. To identify a safe trajectory, you:

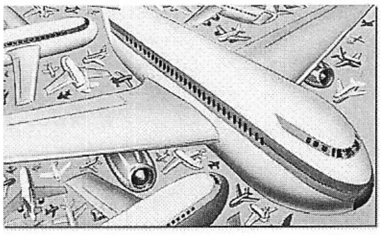

Figure 1

A. must be the team-player, who performs a series of radio-call to coordinate yourself directly with the other pilots to avoid minima violations.
B. must be in radio-contact with air traffic controllers, who constantly monitor minima violations.
C. based on your proved experience, you take your own decisions.

Role-qualification related evidence can be classified as:

A. immediate evidence.
B. direct evidence.
C. indirect evidence.

The EN 5012x represents a standardization framework for:

A. rail domain.
B. medical domain.
C. nuclear domain.

The incomplete identification of potential hazards is related to:

A. epistemic doubt.
B. logical doubt.
C. both.

The "Bow tie" representation may indicate:
A. none of them.
B. FMEA.
C. FTA.

| A | B | C |
|---|---|---|
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 2. Argumentation (7p)

Enumerate at least three types of fallacies (1p).

**Answer:**

Exemplify these three types by providing examples by using GSN/CAE (6p).

**Answer -fallacy type-1 in GSN:**

**Answer - fallacy type-2 in GSN:**

**Answer - fallacy type-3 in CAE:**

## 3. Accident investigation – Wireless Pressure-Sensing Eye Implant (12p)

Consider the following two pieces of information:

1) "The FAA entrusts aviation manufacturers to certify that their own systems comply with air safety regulations. That policy was first ordered by Congress in 2003 as part of efforts to speed up the certification process and reduce costs. The FAA delegated authority to Boeing in 2009, and now allows more than 80 aviation companies to certify their own products' safety."
[https://www.businessinsider.com/faa-change-aviation-safety-oversight-boeing-737-max-crashes-reports-2019-3?r=US&IR=T]

2) "The fatal flaws with Boeing's 737 Max can be traced to a breakdown late in the plane's development, when test pilots, engineers and regulators were left in the dark about a fundamental overhaul (revision) to an automated system that would ultimately play a role in two crashes.

A year before the plane was finished, Boeing made the system more aggressive and riskier. While the original version relied on data from at least two types of sensors, the final version used just one, leaving the system without a critical safeguard. In both doomed flights, pilots struggled as a single damaged sensor sent the planes into irrecoverable nose-dives within minutes, killing 346 people and prompting regulators around the world to ground the Max.

But many people involved in building, testing and approving the system, known as MCAS, said they hadn't fully understood the changes. Current and former employees at Boeing and the Federal Aviation Administration who spoke with The New York Times said they had assumed the system relied on more sensors and would rarely, if ever, activate. Based on those misguided assumptions, many made critical decisions, affecting design, certification and training.

"It doesn't make any sense," said a former test pilot who worked on the Max. "I wish I had the full story."

While prosecutors and lawmakers try to piece together what went wrong, the current and former employees point to the single, fateful decision to change the system, which led to a series of design mistakes and regulatory oversights. As Boeing rushed to get the plane done, many of the employees say, they didn't recognize the importance of the decision. They described a compartmentalized approach, each of them focusing on a small part of the plane. The process left them without a complete view of a critical and ultimately dangerous system.

The company also played down the scope of the system to regulators. Boeing never disclosed the revamp of MCAS to Federal Aviation Administration officials involved in determining pilot training needs, according to three agency officials. When Boeing asked to remove the description of the system from the pilot's manual, the F.A.A. agreed. As a result, most Max pilots did not know about the software until after the first crash, in October."

Taken from: https://www.nytimes.com/2019/06/01/business/boeing-737-max-crash.html

Knowing that a socio-technical system is composed of human-components, organization-components, and technical (hardware/software) components, list at least three of the threats (one related to a human-component, one-related to an organization-component, and one related to a technical-component) that contributed to the occurrence of the accidents and elaborate on them by using the combination of Reason's model & Randell's model. (12p)

**Answer -human component**:

**Answer -organization component**:

**Answer -technical component**:

## 4. Terminological framework related to dependability (6p)

A signal passed at danger (SPAD), also denoted as *running a red signal,* occurs when a train passes a stop signal without authority to do so.
It takes a considerable distance to stop a train. A SPAD often involves a slight or very slight overrun of the signal, at low speed, because the driver has braked too late, often after sighting the signal too late.

In some cases, however, the driver is unaware that they have passed a signal at danger and so continues until a collision occurs, as in the Ladbroke Grove rail crash. In such cases it is up to the safety system to apply the brakes, or for the signaller to alert the driver.

A SPAD may also occur because the signal changed to "danger" too late for the driver to stop before reaching it, due to a technical problem.

An approximate classification for the driver's behaviour is as follows:

Misjudgement
Inattention
Distraction
Fatigue
Misreading of an adjacent signal due to line curvature, or sighting on one beyond
Misunderstanding
Miscommunication
Incomplete or lapsed route knowledge
Acute medical condition (medical emergency), such as a heart attack or stroke
Chronic medical condition, such as sleep apnea causing microsleep

Text adapted from Wikipedia: https://en.wikipedia.org/wiki/Signal_passed_at_danger

a) Make use of the terminological framework related to dependability and to the etiology of accidents to describe at least two different scenarios related to the socio-technical system, which can be extracted from the Wikipedia description given above. 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. Safety case (10p)

Based on your findings (achieved by answering question 4), provide a safety case to show that a train-passenger can safely seat on a train knowing that it is safe enough (SPADs are under control). 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.)