Examination, 7.5 credits, DVA321 – Safety critical systems engineering

Date: 2012-08-31, 8:10–12:30

Responsible teacher(s): Barbara Gallina 021-101631, and Kristina Lundqvist 021-101428. Available to answer questions after 09:30.

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 (6p)

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
Recovery blocks represent: A. a fault forecasting means B. a fault removal means C. a fault tolerance means			
Sanity checks are a means aimed at detecting: A. Value failures B. Timing failures C. Provision failures			
An example of a hazard analysis technique that combines deductive and inductive search strategies is: A. FTA B. HAZOP C. FMECA			
QM is: A. A well-defined ASIL value B. The ASIL value that denotes the lowest safety integrity level C. The ASIL value that denotes the highest safety integrity level			
 This GSN graphical modelling element denotes: A. Nothing (it is not a GSN element) B. An element to be instantiated and developed C. A structure to be developed			
"Incredible" is a well defined value in ISO-26262 w.r.t: A. Controllability B. Severity C. Exposure			

2. Therac-25-failure (8p)

a) Explain what "the Swiss cheese model" is (3p).

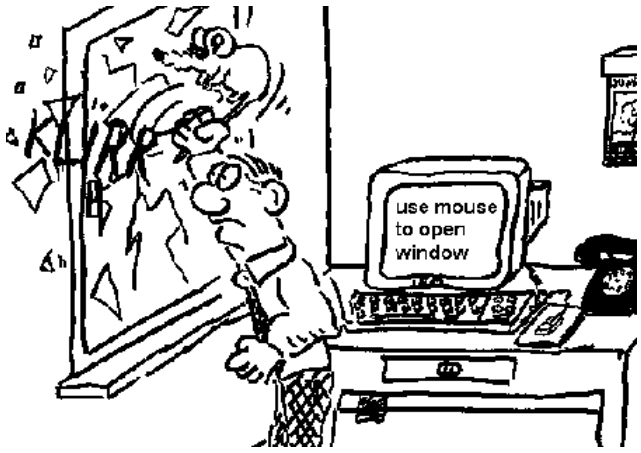
Answer:

b) Using the Swiss cheese model combined with the Randell's model, describe what happened to the Therac-25 (5p).

Answer:

3. Threats (6p)

Given the following picture,



a) identify, if any, the dependability threats (3p);

Answer:

b) discuss and provide adequate counter-measures (3p).

Answer:

4. Worthiness of safety cases (4p)

a) Provide the definition of fallacious appeal (appeal to Improper/Anonymous Authority).

Answer:

b) Provide an example of a paragraph that a regulator would label as a fallacious appeal (appeal to Improper/Anonymous Authority).

Answer:

5. Extended GSN (7p)

a) Draw the graphical representation of the pattern "Hazard avoidance" (2p).

Answer:

b) Then, use the pattern format to define it (5p).

Answer:

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

6. Extended GSN (5p)

a) Draw the graphical representation of the modelling element "Argument contract" (2p).

Answer:

b) Then, discuss the usefulness of *contracts* in safety arguing (3p).

Answer:

7. Hazard analysis techniques (4p)

Provide and explain the template used in FMECA.

Answer: