

Responsible teacher: Barbara Gallina, tel. 021-101631.

NAME:

SURNAME:

PERSONAL NUMBER:

SIGNATURE:

This is an “open book” exam.

**You are expected to provide your answers in this document (by editing it) and then generate a pdf and send it back to: barbara.gallina@mdh.se
Ideally, I should receive one single pdf.**

If for some reasons you want to use other separate sheets and use your hand-writing, make sure that your writing/answers is/are readable, take a picture and insert the picture into the document, alternatively, you are allowed to send separate sheets/files if you cannot merge easily the separate files into a single pdf. However, all of the additional files have to include your name, surname, personal number, signature. Your e-mail must clearly state the number of submitted files.

Max points: 30

Approved: Minimum 15 points

Grade 5: 27 – 30 p

Grade 4: 21 – 26.9 p

Grade 3: 15 – 20.9 p

Grade A: 28 – 30 p

Grade B: 25 – 27.9 p

Grade C: 22 – 24.9 p

Grade D: 18 – 21.9 p

Grade E: 15 – 17.9 p

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. Terminological framework related to dependability (15p)

Robotic surgery

“Surgeon S1 and assisting surgeon S2 could hardly hear each other due to a *"tinny"* sound emanating from the robot console, which S1 was operating. S1 had to shout to warn S2 that the robot was stitching up the valve incorrectly – and then shout again when he saw the robot *"knocked"* one of the surgical assistants' arms.

The robot damaged the patient's aorta, spurting blood everywhere, including the camera it used to *"see."* As events spiraled out of control, the two supervisors – robotics experts normally on hand to take over in a crisis – were nowhere to be found, having gone home part of the way through the procedure.

The surgeons abandoned the now-blind robot and began open chest surgery to repair the tear, but by this point patient's heart was functioning *"very poorly."* The patient died days later of multiple organ failure.

The consultant cardiothoracic surgeon blamed the proctors for leaving early, stating *"The loss of that vital assistance was a major blow at a critical time."* The NHS Trust official read a professor's evaluation of S1 that criticized the decision to move S1 to robotic procedures, calling it *"running before he could walk."* S1 concurred and admitted he had missed multiple training sessions with the robot because he was conducting surgeries elsewhere. Surgeons are supposed to carry out 40 robotic operations on dummies before moving on to patients.

S1 also failed to inform the patient of the added risk of being the UK's first robot surgery patient. According to the consultant anesthetist, S1 knew the proctors were leaving early and chose to continue with the surgery anyway. The consultant anesthetist also claims they ignored his misgivings about how poorly the surgery was going, but that he didn't force the issue as *"it was not my place to harass surgeons."*

The NHS has 60 surgical robots in its hospitals and has operated with robots more than 2,500 times – but never on a mitral valve before. The Coroner said it was *"more likely than not"* that the patient would have survived conventional open heart surgery.

“The Royal College of Surgeons (RCS), responding to the case, said in a statement: “Like the coroner, the RCS recognises the need for much clearer national guidelines on the introduction of new procedures and technologies...It is wholly unacceptable for any surgeon to perform an operation they have not fully trained for.”

“S1 had observed others using the robot and had practised alone on a simulator, but had no individual hands-on training.”

Assume that the pieces of news provide faithful information. Make use of the terminological framework related to dependability and to the etiology of accidents to describe:

- a) what happened (highlight threats, by clarifying the threatened dependability attribute(s), and any eventual causation relationship.

Reminder: do not forget to consider the preliminary concepts related to dependability. Add your own assumptions whenever appropriate and consider human entities, organizational entities and technological entities) (5p)

Answer:

- b) Discuss potential counter-measures, which could have been considered to handle the case described in the pieces of news. Note: you are expected to show your knowledge/skills w.r.t. counter-measures classification by motivating your selection in relation to the scenarios identified in answer a). (5p)

Answer:

- c) Knowing how robotic surgery training should/could work:

“To begin with, **surgeons** will observe experienced colleagues carrying out such procedures. Training on robotics in particular makes use of simulation, as well as other training platforms. Once **surgeons** have completed an appropriate period of observation and simulation, they will move to proctorship where an expert guide will direct them during surgical procedures. They will likely also undertake a fellowship to further develop their skills. For any given operation, **surgeons** need to demonstrate sufficient proficiency and safety before they are allowed to carry it out themselves. Even then, the results should be subject to regular audit and peer review.”

Use the Toulmin model to argue about “S1 was trained enough”. (5p)

Answer:

2 GSN-based argumentation

European Certification and Qualification Association (ECQA) provides a world-wide unified certification schema for numerous professions. To become certified as ECQA Functional Safety Manager a set of skills has to be demonstrated.

The set of skills comprises the following 5 thematic learning units, with 15 elements, each of which has specific ILOs.

1. Introduction to Functional Safety Management
 - a. Introduction to International Safety Standards
 - b. Product Lifecycle
 - c. Terminology used in Functional Safety
2. Management of Functional Safety
 - a. Safety management on organisational and project level
 - b. Safety Requirements and Safety Case Definition**
 - c. Overview of Required Engineering and V&V Methods
 - d. Establish and Maintain Safety Planning
3. Engineering Aspects of Functional Safety
 - a. System Hazard Analysis and Safety Concept
 - b. Integrating Safety in System Design & Test
 - c. Integrating Safety in Hardware Design & Test
 - d. Integrating Safety in Software Design & Test
4. Functional Safety on product and production level
 - a. Integration of Reliability in Design to Enhance Functional Safety
 - b. Safety in the Production, Operation and Maintenance
5. Legal Aspects of Functional Safety
 - a. Legal aspects and Liabilities
 - b. Regulatory & Qualification Requirements

Regarding the unit **Management of Functional Safety**, as also shown in Figure 1, the specific ILOs for the element **Safety Requirements and Safety Case Definition** are:

SAFEUR.U2.E2.PC1 The student is able to identity main elements of safety case, based on standards (e.g. ISO26262, EN50129) and related concepts (assurance case, ISO/IEC 15026)

SAFEUR.U2.E2.PC2 The student is able to establish requirements for evidence collection to construct a safety case

SAFEUR.U2.E2.PC3 The student is able to create necessary arguments and modular safety cases

SAFEUR.U2.E2.PC4 The student is able to explain a safety case for organisational management and other stakeholders (customer, regulator etc.)

SAFEUR.U2.E2.PC5 The student is able to review safety case developed by suppliers or third parties


	
Functional Safety Manager	Functional Safety Manager
Management of Functional Safety	This unit investigates major management aspects of functional safety engineering on organisational and project level. The definition and management of so-called Safety Cases assumes a central role in the functional safety management activities, as safety cases are at the root of modern functional safety engineering methods.
Safety Requirements and Safety Case Definition:	
SAFEUR.U2.E2.PC1	The student is able to identify main elements of safety case, based on standards (e.g. ISO26262, EN50129) and related concepts (assurance case, ISO/IEC 15026)
SAFEUR.U2.E2.PC2	The student is able to establish requirements for evidence collection to construct a safety case
SAFEUR.U2.E2.PC3	The student is able to create necessary arguments and modular safety cases
SAFEUR.U2.E2.PC4	The student is able to explain a safety case for organisational management and other stakeholders (customer, regulator etc.)
SAFEUR.U2.E2.PC5	The student is able to review safety case developed by suppliers or third parties

Figure 1 -ECQA SafeUr ILOs for Safety Requirements and Safety Case Definition

Regarding the unit System Hazard Analysis and Safety Concept, as also shown in Figure 2, the specific ILOs for the element **System Hazard Analysis and Safety Concept** are:

SAFEUR.U3.E1.PC1 The student is able to explain the differences between the standards IEC 61508, ISO 26262 and ISO 13849 regarding their hazard- and risk-analysis.

SAFEUR.U3.E1.PC2 The student is able to explain the terms harm, hazard, hazardous event, severity, exposure, controllability, risk, safety goal, hazard analysis and risk assessment, reasonably foreseeable event. **The student can give examples of his/her own domain.**

SAFEUR.U3.E1.PC3 The student is able to explain an environment in which his system runs and can describe his item definition.

SAFEUR.U3.E1.PC4 The student is able to explain the difference of functional and non-functional behaviour of his system.

SAFEUR.U3.E1.PC5 The student is able to moderate a system analysis and hazard identification. The student is able to provide a template for a development department to give guidelines for the discussion.

Functional Safety Manager	Functional Safety Manager
Engineering aspects of Functional Safety	This unit is the essential complement of Unit 2, i.e., the unit covering the management aspects of functional safety. Its main objective is to bridge the gap between the theoretical standards, and the practical implementation of the latter's rules and requirements. This is considered the main particularity that distinguishes SafeUr from comparable trainings in the same field.
System Hazard Analysis and Safety Concept:	
SAFEUR.U3.E1.PC1	The student is able to explain the differences between the standards IEC 61508, ISO 26262 and ISO 13849 regarding their hazard- and risk-analysis.
SAFEUR.U3.E1.PC2	The student is able to explain the terms harm, hazard, hazardous event, severity, exposure, controllability, risk, safety goal, hazard analysis and risk assessment, reasonably foreseeable event. The student can give examples of his/her own domain.
SAFEUR.U3.E1.PC3	The student is able to explain an environment in which his system runs and can describe his item definition.
SAFEUR.U3.E1.PC4	The student is able to explain the difference of functional and non functional behaviour of his system.
SAFEUR.U3.E1.PC5	The student is able to moderate a system analysis and hazard identification. The student is able to provide a template for a development department to give guidelines for the discussion.

Figure 2 ECQA SafeUr ILOs for System Hazard Analysis and Safety Concept

a) Use GSN and Argue about:

“A student who achieves DVA437 ILOs is ready to show achievement of SafeUr ILOs.”

Note: you are expected to use GSN patterns where appropriate. (5p)

Answer:

b) Then, use GSN to argue about: “I am ready to take the ECQA SafeUr exam regarding unit 2, element 2 (Safety Requirements and Safety Case Definition)”

XOR

“I am ready to take the ECQA SafeUr exam regarding unit 3, element 1 (System Hazard Analysis and Safety Concept)”

Note: Do not forget, that

1-your argument may contain assumptions.

2-an argumentation must be founded. Thus, in addition to the pointers to the evidence, you are also expected to include the evidence-artefacts about your acquired knowledge in relation to the ILOs of that unit (at least 1 evidence artefact shall be provided. You are free to choose.). (5 p)

Answer:

c) As you know, while arguing, one may introduce fallacies. Consider your GSN-argument, provided in the previous question (2.b), choose at least 2 fallacies, and discuss about their presence or absence in your argument. (5p)

Answer: