Module Code
COM00173M

MSc, MEng Degree Examinations 2023-4

DEPARTMENT OF COMPUTER SCIENCE

High-Integrity Systems Engineering (HINT)

Open Assessment 1

Open Individual Assessment

Issued: Thursday 5th October, 2023 Midday (S1/2/Thur)
Submission due: Thursday 16th November, 2023 Midday (S1/7/Thur)
Feedback and marks due: Thursday 21st December, 2023 (S1/Vac 1/Thur)

All students should submit their answers through the electronic submission system: http://www.cs.york.ac.uk/student/assessment/submit/ by Thursday 16th November, 2023 Midday (S1/7/Thur). An assessment that has been submitted after this deadline will be marked initially as if it had been handed in on time, but the Board of Examiners will normally apply a lateness penalty.

Your attention is drawn to the section about Academic Misconduct in your Departmental Handbook: https://www.cs.york.ac.uk/student/handbook/.

Any queries on this assessment should be addressed by email to Iain Bate at iain.bate@york.ac.uk. Answers that apply to all students will be posted on the VLE.

Your exam number should be on the front cover of your assessment. You should not be otherwise identified anywhere on your submission.

Any queries about this assessment received within 7 calendar days of the submission deadline will not be answered.

You have been tasked with introducing a state of the art communications system into an aircraft where the current network technology is based on the highly-predictable ARINC 629. The current system connects a number of high-criticality systems that have tightly controlled message passing in terms of the period and amount of data. The current system is however reaching its capacity and is one of many communications system on the aircraft. Management have been told that Time-Sensitive Networks based on the Ethernet protocol could give significant benefits including the following.

1. Weight - A number of communications systems that each have their own cabling could be replaced by one system with one set of cables.

2. Capacity - Even a 100 Mbit/second ethernet-based system would give much more bandwidth than all the existing systems put together.

3. Cost - Having one communication system would significantly reduce the design costs.

4. Flexibility - The ability of more systems with different criticality levels to safely and securely share information would add significant flexibility.

Your task is to investigate Time-Sensitive Networks based on the Ethernet protocol to understand its capabilities, the benefits and drawbacks, and the potential implications on safety. Time-Sensitive Networks are a new emerging technology and standards primarily targeted at safety-critical systems. There are many different uses of the term Time-Sensitive Network in the literature, however the starting point is the wikipedia article found at https://en.wikipedia.org/wiki/Time-Sensitive_Networking.

The findings will be shared with other companies so you should not use your own companies specific systems in the study as they would contain valuable intellectual property. Therefore during this process, you do not need to consider all systems on the aircraft. Instead you could consider the critical systems communication problem through public domain examples or through a general problem such as a system with the following sub-systems.

1. Flight Control System - Development Assurance Level (DAL) A

2. Engine Control System - DAL A

3. Navigation System - DAL B

4. Power Distributed System - DAL B

5. Waste Management System - DAL C

6. Infotainment System - DAL E

7. Fuel Management System - DAL C

The output that is expected is a 12 page report in 11 point font. The 12 pages should include all figures and tables although extra pages can be used for references.

Throughout your answers to the following questions, please state any further assumptions needed.

Question 1 (30 marks)

Perform an assessment of the technologies including the following.

- Q1(A) - An explanation of Ethernet system to understand the protocol and its management of resources (5 marks).
- Q1(B) - An explanation of both the industrial application and academic research of Time-Sensitive Networks (15 marks). The answer should consider temporal predictability of systems that use it and its ability to support system fault tolerance.
- Q1(C) - An illustration of how a mixed-criticality system could be configured to use a Time-Sensitive Network (10 marks). The answer should consider how temporal budgets could be managed and analysed to show that they are met.

Question 2 (40 marks)

Perform a failure analysis of the system presented in Q1(C) using fault tree analysis to illustrate how failures in the communications system could lead to hazardous effects.

- Q2(A) - Present a suitable fault tree analysis with clear traceability to the model and components in Q1(C) (10 marks).
- Q2(B) - Explain the fault tree analysis (15 marks). The explanation should discuss the contribution of failures of the communication system to the overall top-level event and the lower predictability that may exist with lower-criticality systems connected to the communications system.
- Q2(C) - Explain how the management and analysis approaches of Time-Sensitive Networks may help reduce the likelihood of the top-level event in the fault tree (15 marks). The answer should consider how temporal budgets help reduce the likelihood of failures and enable fault tolerance.

Question 3 (30 marks)

Produce a safety argument using Goal Structuring Notation with the top-level claim being that a hazard is sufficiently mitigated.

- Q3(A) - Present the safety argument with clear traceability to the model and components in Q2(A) (10 marks)

- Q3(B) - Explain the safety argument (10 marks). The explanation should discuss how it has been derived including why you consider it to be correct and the insight gained from it.
- Q3(C) - Define specific techniques that will gather the evidence to support the claims at the bottom level of the argument can be gathered (10 marks). The explanation should discuss any challenges that are expected when gathering the evidence.

End of examination paper