University of Glasgow | School of Computing Science

Assessed Coursework

Course Name	Safety Critical Systems M			
Coursework Number	1			
Deadline	Time:	4.30pm	Date:	11th March 2016
% Contribution to final course mark	20%			
Solo or Group ✓	Solo	✓	Group	
Anticipated Hours				
Submission Instructions				
Please Note: This Coursework cannot be Re-Assessed				

Code of Assessment Rules for Coursework Submission

Deadlines for the submission of coursework which is to be formally assessed will be published in course documentation, and work which is submitted later than the deadline will be subject to penalty as set out below. The primary grade and secondary band awarded for coursework which is submitted after the published deadline will be calculated as follows:

(i) in respect of work submitted not more than five working days after the deadline
  a. the work will be assessed in the usual way;
  b. the primary grade and secondary band so determined will then be reduced by two secondary bands for each working day (or part of a working day) the work was submitted late.

(ii) work submitted more than five working days after the deadline will be awarded Grade H.

Penalties for late submission of coursework will not be imposed if good cause is established for the late submission. You should submit documents supporting good cause via MyCampus.

Penalty for non-adherence to Submission Instructions is 2 bands

You must complete an "Own Work" form via https://studentltc.dcs.gla.ac.uk/ for all coursework

Safety-Critical Systems: Open Assessment 2015-16

Software Safety and Cyber Security in Aviation (Level M)

Prof. Chris Johnson
School. of Computing Science, University of Glasgow, Glasgow, G12 8QQ. Scotland.
johnson@dcs.gla.ac.uk, http://www.dcs.gla.ac.uk/~johnson

1 Introduction

There are many well-understood techniques for increasing the safety of software in aviation – some are encoded in standards such as ED-153 (ground based systems) and DO-178C (airborne). The overall approaches are similar to those covering functional safety in IEC61508 but there are many detailed differences, for instance 178C focuses on traceability. These approaches were developed at a time before we understood the potential risks from safety that are associated with cyber-attacks on aviation infrastructures. Software cyber-security standards, such as the ISO 27k series, can help but they have almost nothing to say about safety concerns.

2 Tool Development

Your task in the open assessment is to develop a technique that will help identify the safety-related hazards that arise from cyber-security threats in aviation. The aim is to enable senior or middle management to assess and mitigate the impact that a cyber attack might have on safety-related aviation systems – either omn the ground in air traffic management or in airborne systems. Beware: the threats that you consider must be credible and justified. The design of the technique is entirely open. You may choose to use one of the risk assessment techniques that are introduced during this course, such as Fault Trees or Failure Modes, Effects and Criticality Analysis combined with security techniques, such as Attack Trees. Alternatively, you may choose to develop an entirely new approach. However, if you use an existing approach you must show how it can be used with specific examples of security threats to aviation infrastructures.

The key aim is to help organizations assess the likelihood and consequence of threats that can arise in aviation systems. There have been numerous studies on these issues but this is a very open area allowing scope for creativity and design. It is VITAL that your answer should contain a detailed case study based on existing research.

You may choose to develop electronic tools that support the application of your technique using any programming methodology. The implementation of the tool could rely on simple web pages generated using HTML, PHP or any other associated technology. Your design may be realized using conventional programming languages or you could simply rely on paper-based support. However, the marking scheme will take into account both the strengths of the design for the risk assessment technique and the effectiveness of an implementation in terms of the support that they offer to the potential end-users.

3 Evaluation

It is important that you evaluate your technique/tool for assessing the cyber-security risks for aviation safety. One means of doing this would be to ask a number of different users to try it out, exploiting an appropriate evaluation methodology. For example, you could ask one group to use your technique and another to use an alternate approach developed by someone else in the course. If you do this you MUST consider the relevant plagiarism guidance on the School Learning and Teaching Committee web site and state the name of the person you worked with on your submission. You must develop your reports independent of each other. You also need to consider the level of existing expertise that test participants will have in safety-critical software development.

If you split your users into two groups (one for your tool and the other for your friends) then this raises important methodological concerns. Firstly, how would you insure that both groups have the same level of expertise and background knowledge so that any comparisons are fair? Secondly, how would you go about assessing the accuracy of any risk assessments that are produced? Please consult with me before conducting your evaluation so that I can provide advice in answering some of these questions. You should also consult the course handbook and associated web pages that cover the ethical guidelines for user testing.

4 Transferable Skills

This exercise will provide a first-hand introduction to the challenges that face many large organizations, airlines, regulators, infrastructure operators, as they develop aviation software – remember that software also control physical security through airport CCTV cameras, screening and access control systems etc. There is little agreement on the best approaches to adopt and hence you will be working in an area of active research, which is also a focus for public, government and commercial interest.

5 Assessment Criteria and Submission Details

This exercise is degree assessed. It contributes 20% to the total marks associated with this course. The body of the report should not exceed fifteen A4 pages. The report must be printed out and must be submitted in a secure binder (something that keeps the pages together and does not have sharp edges). It must include: A title page containing your contact details (metric, email etc); a table of contents and appropriate page numbers; a section on the tool that you developed; a section on the evaluation method that you used; a results sections and some conclusions.

In addition to the fifteen pages in the body of the report, you may also include appendices. These should contain the listing of any code used during the study together (this can be included on a CD) with suitable acknowledgements for the source of code that has been borrowed from other programmers. The report should be handed in by 16:30, 11th March 2016 using the submission box outside the teaching office in Lilybank Gardens. Please make sure that you keep back-up copies of all of your work and submit a plagiarism statement using the standard on-line form. The following marking scheme will be applied: 30 for the method; 20 for the results; 30 for the conclusion; 20 for the technical documentation. All solutions must be the work of the individual submitting the exercise and the usual lateness penalties will apply unless I am given good reason in advance of the deadline. *You must state the title of this question on the front of your submission so I know you are answering the level M open exercise.*

6 Hints

You will need to do considerable reading first so please do not delay starting this assessment.