University of Glasgow | School of Computing Science

Assessed Coursework

Course Name	**Safety Critical Systems M**			
Coursework Number	**1**			
Deadline	**Time:**	**4.30pm**	**Date:**	**16/3/2018**
% Contribution to final course mark	**20%**			
Solo or Group ✓	**Solo**	✓	**Group**	
Anticipated Hours				
Submission Instructions	**Submit to the secure box outside the Teaching Office, Room F161, School of Computing Science, Lilybank Gardens.**			
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 2017-18

Supporting the Regulation of Cyber Security in Safety-Critical Systems (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

The UK Health and Safety Executive published the first guidance for its inspectors in assessing the cyber security of safety-critical industrial control systems in 2017[1]. This guidance is particularly important in the aftermath of attacks, such as those on the Ukrainian infrastructures (2016-17) and the Stuxnet or Olympic Games attacks on Iran. This exercise is intended to build on the HSE guidance by developing tools that will help either a) inspectors to audit companies using the guide or b) companies preparing for a visit by an HSE inspector considering the cyber security of safety-critical systems.

2 Tool Development

Your task in the open assessment is to develop a technique that will support the application of the new HSE guidance. It follows a high-level, process based approach similar to that covered in the course for IEC 61508. In consequence, there is a need for tools that can be used by inspectors or by companies to show whether or not a particular system/process/operation meets the requirements embedded within the document.

The design of the technique or tool support is entirely open. You may choose to support particular stages of the process recommended in the guidance (see HSE Figure 1, page 6). For instance, by using one of the risk assessment techniques that are introduced during this course, such as Fault Trees or Failure Modes, Effects and Criticality Analysis for cyber related concerns in a safety-critical process. Alternatively, you may choose to develop an entirely new approach. In both cases, you must illustrate the application of the approach to support the regulation of cyber security in safety-critical systems. Or put more simply, you must demonstrate that the tool helps someone to convince government that a safety-critical system is sufficiently robust against cyber threats. It is VITAL that your answer should contain a detailed case study.

It is up to you if you want to develop paper-based or electronic solutions. Tools might be implemented using HTML, PHP or any other associated technology. The marking scheme will take into account both the strengths of the design and the effectiveness of an implementation in terms of the support that they offer to the potential end users (regulated companies or HSE inspectors).

3 Evaluation

It is important that you evaluate your technique/tool to support the regulation of cyber security in safety critical systems. One means of doing this would be to ask a number of different users to try it out, taking on the role of either the company being inspected or of the HSE inspector. You will need to exploit 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 the regulation of safety critical systems.

[1] http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf, last accessed January 2018

If you split your users into two groups for each tool 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 results that are produced using your tool? 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 both companies and government regulators who are working together to protect the cyber security of safety critical systems. There is little common 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 on 16/3/2018 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. General information about the regulatory regime for Health and Safety in the UK is available on http://www.hse.gov.uk/pubns/hse49.pdf.