University of Glasgow | School of Computing Science

Assessed Coursework

Course Name	**Safety-Critical Systems 4**			
Coursework Number	**1**			
Deadline	**Time:**	**09.00**	**Date:**	**24th November 2011**
% Contribution to final course mark	**30%**			
Solo or Group ✓	**Solo**	✓	**Group**	
Anticipated Hours	**Open ended but minimum estimate 20 hours**			
Submission Instructions	**Via locked box outside the teaching office.**			
Please Note: This Coursework cannot be Re-Done				

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://webapps.dcs.gla.ac.uk/ETHICS for all coursework UNLESS submitted via Moodle

Safety-Critical Systems: Open Assessment 2011-2012

Safety Risk Assessments and Cyber Security

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

1 Introduction

In this course you will meet a number of 'leading' techniques for risk assessment, including FMECA, Fault Trees, HAZOPS. You will also be introduced to safety cases and the GSN approach that can be used to map out arguments about why a system is acceptably safe, using the results of these risk assessment techniques.

The traditional focus of these techniques has been to identify hazards and then mitigate the risks associated with them. However, they cannot easily be used to model security threats. This is important because a deliberate cyber-attack could have significant consequences for the safety of many critical systems. The attack could coincide with other more 'typical' hardware and software failures or an adversary could exploit the opportunities provided by such failures to launch a directed attack. The purpose of this open assessment is to develop an integrated technique to support the risk assessment of both security threats and safety hazards. You must then apply the technique to a case study of your choice. You may or may not choose to develop a software tool to support the user of your approach, however, such support is likely to attract additional marks.

2 Tool Development

Your task in the open assessment is to develop a technique that will help companies to mitigate the impact of cyber-attacks on the safety of systems that they operate. The aim is to enable senior or middle management to assess the safety related risks that are associated with a potential attack. 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. Alternatively, you may choose to develop an entirely new approach. The key aim is to help organizations assess the likelihood and consequence of hazards that can arise during cyber-attacks both from inside or outside that company. The specific focus must be on identifying safety related risks and ideally to help managers mitigate those risks by appropriate planning before an attack takes place.

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 integrated security and safety risk assessments. 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 one of the alternate approaches sketched in [1, 2, 3]. However, 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 as they prepare for cyber-attacks. For more information on the nature of the threats that we face, please look at the Centre for the Protection of National Infrastructures web site (www.cpni.gov.uk) as well as a draft paper [4]. 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. The exercise will provide some understanding of the problems that can arise in preparing for low probability, high-consequence events. It will also underline the uncertainty that often characterizes risk assessment in safety-critical engineering. Many of the skills provided by this assessed exercise are in scarce supply.

5 Assessment Criteria and Submission Details

This exercise is degree assessed. It contributes 30% 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. It must include:

- A title page containing your contact details (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.
- 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 with suitable acknowledgements for the source of code that has been borrowed from other programmers. The report should be handed in by 9am on Thursday 24th November 2011; I will confirm the details in a lecture before the deadline. 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: 15 for the method; 10 for the results; 15 for the conclusion; 10 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.

References

[1] C.W. Johnson, CyberSafety: On the Interactions Between CyberSecurity and the Software Engineering of Safety-Critical Systems. Draft available from: http://www.dcs.gla.ac.uk/~johnson/papers/IET_2011/CyberSafety.pdf

[2] C.W. Johnson, Using Assurance Cases and Boolean Logic Driven Markov Processes to Formalise Cyber Security Concerns for Safety-Critical Interaction with Global Navigation Satellite Systems, in J. Bowen and S. Reeves(eds.), Proceedings of the 4th Formal Methods for Interactive Systems Workshop 2011, Limerick, Ireland, keynote address, 2011. Available on: http://www.dcs.gla.ac.uk/~johnson/papers/FMIS2011/Chris.pdf

[3] C.W. Johnson and A. Atencia Yepez, Mapping the Impact of Security Threats on Safety-Critical Global Navigation Satellite Systems. In C.G. Muniak (ed.), Proceedings of the 29th International Systems Safety Society, Las Vegas, USA 2011, International Systems Safety Society, Unionville, VA, USA, 2011. Available on: http://www.dcs.gla.ac.uk/~johnson/papers/ISSC2011/Space_Security_Cases.pdf

[4] C.W. Johnson, Anti-Social Networking: Crowdsourcing and the CyberDefence of National Critical Infrastructures. In G. Grote, M. Bourrier, B. Fahlbruch and G. Motet (eds.), Proceedings of the New Technologies and Work Network, Toulouse, France, 2011. Available on: http://www.dcs.gla.ac.uk/~johnson/papers/Gudela/Cyberdefence_And_Anti_Social_Networking.pdf