



## Assessed Coursework

<b>Course Name</b>	Safety Critical Systems 4		
<b>Coursework Number</b>	1		
<b>Deadline</b>	<b>Time:</b>	4:30pm	<b>Date:</b> 6 <sup>th</sup> March 2015
<b>% Contribution to final course mark</b>	20	<b>This should take this many hours:</b>	
<b>Solo or Group</b> ✓	<b>Solo</b> ✓	<b>Group</b>	
<b>Submission Instructions</b>	Submit into the secure box provided outside the Teaching Office, Room F161, Lilybank Gardens		
<b>Who Will Mark This?</b> ✓	<b>Lecturer</b> ✓	<b>Tutor</b>	<b>Other</b>
<b>Feedback Type?</b> ✓	<b>Written</b>	<b>Oral</b>	<b>Both</b> ✓
<b>Individual or Generic?</b> ✓	<b>Generic</b>	<b>Individual</b>	<b>Both</b>
<b>Other Feedback Notes</b>			
<b>Discussion in Class?</b> ✓	<b>Yes</b>	<b>No</b>	
<b>Please Note: This Coursework cannot be Re-Done</b>			

### 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

<http://www.dcs.gla.ac.uk/socs-online> for all coursework

**UNLESS submitted via Moodle**

# Identifying the Major Software Safety Concerns in Driverless Cars (Level 4)

Prof. Chris Johnson

School. of Computing Science, University of Glasgow, Glasgow, G12 8RZ. Scotland.  
johnson@dcs.gla.ac.uk, <http://www.dcs.gla.ac.uk/~johnson>

## 1 Introduction

Projects such as the Google Self-Driving Car with the associated Google Chauffeur software and the General Motors EN-V raise enormous questions about the design, implementation, verification and validation, certification, operation and maintenance of driverless vehicles. These concerns partially explain the limited success of previous projects stretching back to CMU's Navlab/ALV or Mercedes Prometheus.

## 2 Tool Development

Your task in the open assessment is to develop a technique that will help identify address any of the concerns that arise from the application of autonomous software control to a driverless vehicle. The aim is to enable senior or middle management at least one of the stakeholder organisations to assess and mitigate software safety related risks. Stakeholders in this context include, but are not limited to, autonomous vehicle manufacturers, conventional vehicle manufacturers, other road users, regulators, road-safety organisations, police agencies. 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. However, if you use an existing approach you must show how it can be used with detailed AND specific case studies based on significant research into existing plans by manufacturers/governments that have approved these vehicles for trial use on their roads.

The key aim is to help organizations assess the likelihood and consequence of hazards that can arise from the integration of autonomous software into road vehicles. These include issues associated with testing and debugging, especially from the risk exposure associated with mass-market products. For more on this you might look at the previous recalls of conventional vehicles in response to software concerns. You must consider at least one third party hazard; this is covered in the second lecture of the course. The specific focus must be on helping managers mitigate those risks by appropriate planning before the vehicle is operated outside of a lab.

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 associated with autonomous software in driverless vehicles. 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 the people you test will have in the development of autonomous road vehicles.

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 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 try to innovate and at the same time ensure the safety of their products. 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 underline the uncertainty that often characterizes risk assessment in safety-critical engineering – for example, credible attempts to use quantitative techniques will attract high marks especially if you can validate assessments of the probability and consequence of particular hazards. You should consider the role of regulators in the development process; this is covered in the early part of the course including the use of process based software standards. Recall also that regulators must protect safety but also, where possible, enable companies to develop new markets.

#### **5 Assessment Criteria and Submission Details**

This exercise is degree assessed. It contributes 20% to the total marks associated with this course – see the associated warnings on Moodle. 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 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 9am on 6<sup>th</sup> March 2015 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 your name and the title of the exercise on the front of your submission so I know this is level 4 and a level M open exercise.*

#### **6 Hints**

You will need to do considerable reading first into the background of autonomous road vehicles so please do not delay starting this assessment.