Safety-Critical Systems: Open Assessment 2004-2005

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

1 Introduction

Safety cases are an important part of the regulatory environment in the UK and many other countries. The IEE define a safety case to be "A documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment":

`http://www.iee.org/oncomms/pn/functionalsafety/safety_cases.cfm`

Several industries require the use of safety cases before companies can begin operating. For instance, the Railways (Safety Case) Regulations 2000 require those providing railway infrastructure or operating train services to submit a safety case detailing: their safety policies; a risk assessment for their operations; an overview of their safety management systems and, finally, any risk control measures. The UK Health and Safety Executive's policy on the assessment of these safety cases can be found on:

`http://www.hse.gov.uk/railways/rsc.htm`

There are two parts to this exercise. The first is to devise a tool to assist in the development of a safety case. The second is to evaluate the usefulness of your tool against one or more case studies.

2 Tool development

You are free to use any implementation techniques during the development of your analytical tools. These could simply focus on the development of html guidance on existing techniques, such as the Adelard Safety Case Development (ASCAD)[1] notation or Tim Kelly's Goal Structuring Notation (GSN). Both of these techniques are referenced from the IEE site, mentioned above. For instance, client side image maps could provide a means of linking from a GSN diagram to supporting documents about the safety of an example system. Alternatively, you might re-use existing AWT/Swing code on the web to develop a simple diagram editor for GSN or elements of the ASCAD approach. You might even prefer to develop your own approach or to alter some of the existing techniques.

3 Evaluation

It is important that you attempt to evaluate your support for safety case development. One means of doing this would be to ask a number of different 'analysts' or users to exploit your tool during an initial case study. For instance, two groups might be asked to sketch out a safety case for a simplified example. One group might be asked to do

[1] Adelard already provide tool support for ASCAD, you should ideally extend support beyond that already offered.

this with the support of your tool while another might be set the same task but without access to your system. 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 can be fairly made? Secondly, how would you go about assessing the quality of the arguments that each group develops? Please consult with me before conducting your evaluation so that I can provide advice in answering some of these questions.

4 Transferable Skills

This exercise will provide a first-hand introduction to the safety cases that underpin the operation and regulation of systems across a broad range of industries. The development of tool support will also provide some understanding of the problems that can arise when trying to apply existing safety case techniques. These areas are the subject of continuing research. In particular, regulatory and commercial organisations are only just beginning to understand the problems posed by the development of safety cases for new generations of computer-related systems. Hence many of the skills provided by this assessed exercise are in very 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. ¡P¿ The report should be handed in at the start of the lecture on Friday 26th November 2004. Extensions will only be granted in exceptions circumstances and they should be requested as soon as possible. Extensions for equipment failures may be granted provided that you let me know as soon as they occur so that I can have them fixed as soon as possible. Please make sure that you keep back-up copies of all of your work. 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 plagiarism form must be attached to all solutions. All questions about this exercise should be addressed to Chris Johnson.