Safety-Critical Systems: Open Assessment 2013-14

Recovery from Software Failures (Level 4)

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

After software failure causes the loss of a safety-related service, organisations must work hard to ensure that an application is acceptably safe to operate. The failure may be transient, in which case it will not recur or it could be intermittent, happening again at a later date. Key issues that arise include how much money to spend to identify the causes of failure when a software application seems to be operating correctly again. Even if we think we have found the cause of a bug then there may be other failure modes that we have not discovered – how can we be sure it is safe to start again?

2 Tool Development

Your task in the open assessment is to develop a technique that will help identify the hazards that arise from restarting a safety-related service after a major software failure. The aim is to enable senior or middle management to assess and mitigate the safety related risks. 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 specific examples of the recovery from major failures in existing infrastructures.

The key aim is to help organizations assess the likelihood and consequence of hazards that can arise in restarting safety-related services following software failures. These include confidence in the diagnosis of failure modes, they also include issues associated with testing and debugging and with the use of fall back systems in case things go wrong. You can choose to develop tools and techniques that address all of these hazards or that focus on one particular set of concerns. However, 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 an the software is restarted.

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 risks during recovery from major failures. 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 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 each develop your reports independent of each other. You also need to consider the level of existing expertise that the people you test on will have in these sorts of recovery tasks.

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 recover from software failures. 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. You should consider the role of regulators in the recovery process; this is covered in the early part of the course including the use of process based software standards.

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. 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 Wedneday 27th November 2013 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: 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. *You must state the title of this question on the front of your submission so I know which group you belong to.*

6 Hints

There are a number of well-known incidents that can be used to inform your work – an example would be the Dublin Airport LAN failure (lecture 11, on the course web page) or the response to the Ueberlingen accident mentioned in the notes:

http://www.dcs.gla.ac.uk/~johnson/papers/EUROCONTROL_RD_Ueberlingen.pdf

Alternatively, you could look at some of the NHS and other healthcare incidents, see for instance:

http://www.dcs.gla.ac.uk/~johnson/papers/AHRQ/case_study.pdf

You will need to do considerable reading first into the background of a software related failure so please do not delay starting this assessment.