Safety-Critical Systems: Open Assessment 2008-2009

Safety Assessments for Energy 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

The UK is increasingly concerned about the security and reliability of energy supplies. This is a concern that is shared with many other countries in Europe. There are dwindling supplies of fossil fuels and those reserves that are being opened up are now either extremely expensive to exploit or are located in regions that are associated with a degree of political instability or are in areas that may be considered as political and economic rivals. These pressures are exerting themselves at a time of increasing demand for energy by a growing number of developing countries. Domestic demand in Europe and the UK is also rising. Natural events have also affected energy markets, tropical storms in the Gulf of Mexico, have further reduced limited refining capacity and have increased prices across the energy markets. Within the UK, we have aging infrastructures, especially in terms of electricity generation, and the North Sea reserves can no longer be relied upon as a 'strategic buffer' to provide additional supplies in times of crisis. The uncertain mix between renewable, nuclear and conventional power supplies also creates problems of maintaining strategic power reserves.

Interruptions to power supplies have a host of economic, social and political consequences. One aspect of this is the hazards that arise during blackouts. There are vulnerable groups in the community – including those with medical conditions that rely on devices in their own homes to manage a growing range of medical conditions. There are knock-on effects on critical infrastructures, previous blackouts in Italy and North America have left hundreds of thousands of people trapped on trains [1]. Power to water treatment plants, to road signs, to air traffic control infrastructures may also be lost [2]. Your task is to help companies plan for these hazards and mitigate their consequences to their employees or to the general public.

2. Tool Development

The aim of this open assessment is to develop a tool that will help companies plan for the risks to safety that may arise through energy insecurity in the next 5 to 10 years. Your tool should enable senior or middle management to assess the safety related risks that are associated with the loss of energy infrastructures. The design of the tool 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 extend other approaches such as HAZOPs, or to develop entirely new techniques. The key aim is to help organizations assess the likelihood and consequence of hazards that are associated with black outs. The specific focus must be on identifying safety related risks and ideally to help managers mitigate those risks by appropriate planning before a contingency occurs.

Just as the design of the risk assessment tool is open, you are also free to use any technologies to support the implementation of your approach. 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. However, the marking scheme will take into account both the strengths of the design and the effectiveness of the implementation in terms of the support that they offer to the potential end users.

3. Evaluation

It is important that you evaluate your tool for safety risk assessment. One means of doing this would be to ask a number of different users to try it out. For instance, one group might be asked to use an electronic risk assessment tool while another uses a paper based form. 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 changes in the domestic and international energy markets. 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 on Thursday 27th November 2008 using the secured boxes in Lilybank Gardens. Please make sure that you keep back-up copies of all of your work and include a plagiarism statement using the standard 'pink 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 plagiarism form must be attached to all solutions.

References

[1] C.W. Johnson, Understanding Failures in International Infrastructures: A Comparison of Major Blackouts in North America and Europe. In R.J. Simmons and D.J. Mohan and M. Mullane, Proceedings of the 26th International Conference on Systems Safety, Vancouver, Canada 2008, International Systems Safety Society, Unionville, VA, USA, ISBN 0-9721385-8-7, 2008. http://www.dcs.gla.ac.uk/~johnson/papers/Blackout_Comparison/Johnson_Power_Infrastructure.pdf, last downloaded 8th Oct. 2008.

[2] C.W. Johnson, G. Amar, T. Licu and R. Lawrence, High-Level Architectures for Contingency Planning in Air Traffic Management. In R.J. Simmons and D.J. Mohan and M. Mullane, Proceedings of the 26th International Conference on Systems Safety, Vancouver, Canada 2008, International Systems Safety Society, Unionville, VA, USA, ISBN 0-9721385-8-7, 2008. Available on: http://www.dcs.gla.ac.uk/~johnson/papers/Contingency/johnson_Contingency.pdf, last downloaded 8th Oct. 2008.