Safety-Critical Systems: Open Assessment 2018-19

Supporting Competent Authorities in the Implementation of the NIS Directive for Safety-Critical Industries (Level M)

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

The Network and Information Systems Directive has been integrated into UK law[1]. As part of this, the Operators of Essential Services (OES) are expected to be guided and to some extent assessed by Competent Authorities (CAs). For example, airlines operating UK flights will be supported by the Civil Aviation Authority acting as the Competent Authority. In UK energy distribution, the Competent Authority is the Health and Safety Executive (HSE).

The aim of the directive is to increase the resilience of critical infrastructures and, in particular, improve the robustness of systems that rely on the exchange of digital information. In most cases, the loss of these infrastructures can have an impact on safety-related applications. This has resulted in many CAs being drawn from the regulatory agencies that protected the safety of complex systems and they have had to extend their competence to consider the cyber security of critical infrastructures.

2 Tool Development

Your task in the open assessment is to develop a technique that will help CAs meet their requirements under new NIS Directive. For example, there is a need for tools that can be used by inspectors or by companies to show whether or not a particular system/process/operation meets reliability requirements. For more detailed information on the techniques that might be used by a CA to meet the NIS Directive requirements see the HSE guidance on Cyber Security for Industrial Automation and Control Systems[2].

The design of the technique or tool support is entirely open. For instance, you might extend the use of one of the risk assessment techniques that are introduced during this course, such as Fault Trees or Failure Modes, Effects and Criticality Analysis for cyber related concerns in a safety-critical process. Alternatively, you may choose to develop an entirely new approach. In both cases, you must illustrate the application of the approach to support the regulation of cyber security in safety-critical systems, within the scope of the NIS Directive. Or put more simply, you must demonstrate that the tool helps someone to convince government that a safety-critical system is sufficiently robust. It is VITAL that your answer should contain a detailed case study so you should begin by selected and reading about an industry covered by the UK implementation of the Directive[3].

It is up to you if you want to develop paper-based or electronic solutions. Tools might be implemented using HTML, PHP or any other associated technology. The marking scheme will take into account both the strengths of the design and the effectiveness of an implementation in terms of the support that they offer to the potential end users (Competent Authorities as defined within the NIS Directive).

---

[1] https://www.ncsc.gov.uk/guidance/introduction-nis-directive
[2] http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf
[3] https://www.gov.uk/government/consultations/consultation-on-the-security-of-network-and-information-systems-directive

3 Evaluation

It is important that you evaluate your technique/tool to support the application of the NIS Directive for safety critical systems. One means of doing this would be to ask a number of different users to try it out, taking on the role of the Competent Authority. You will need to exploit 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 test participants will have in the regulation of safety critical systems.

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 both companies and government regulators who are working together to protect the cyber security of safety critical systems. 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.

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 (something that keeps the pages together and does not have sharp edges). It must include: a title page containing your contact details (metric, 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 16.30 on 27th February 2019 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 the title of this question on the front of your submission so I know you are answering the level M open exercise.

You will need to do considerable reading first so please do not delay starting this assessment.