File 20100118.0730: Notes from meeting with Dr Martin this morning:

I have been expanding the methodology chapter outline, reading papers in the safety critical software literature in search of axioms and principles, and thinking about how to design a survey (*pace* Dr Jirotka) using SurveyMonkey to divine what wider a group of practitioners (probably larger, and distinct from the participants in my case studies) think about the connection between defence-in-depth and CT&E. I mentioned to Dr Martin that I think this will provide a useful orthogonal bit of information, not obtainable from the case studies or interviews with participants in the first case study. I have been working on writing the introduction. Dr Martin indicated that my writing style is okay and the level of detail is good. Keep expanding the outline.

With regard to safety critical axioms and principles, I found lots on architecturl principles and design principles, but not so much on te philosophy of testing or what appropriate levels of testing are. Dr Martin said that one of the favourite principles of safety critical writers is ALARP: As Low As Rasonably Possible. Look at the book *Safeware* by Leveson for principles. If that textbook doesn't contain a list of principles, axioms, or theorems, then there probably aren't any. (The book is on order from Amazon right now.)

Dr Martin questioned the connection between defence-in-depth and level of testing in people's minds. Wondering if it is really there or not. Defence in depth is a principle honoured. 'There is this whole continuum of testing, validation, IV&V, certification, . . . '. '. . . poorly explored rationale. . . ' *Do people really have a rationale for where they sit on this continuum?* Dr Martin says there are few studies of whether Formal Methods actually help.

Random thoughts: process depth instead of test depth. Unit tests. Test coverage.

We discussed the idea back and forth for a while and Dr Martin pulled a few books off the shelf behind him. I mentioned the paper by Bowen and Stavridou [1] but I haven't finished reading it yet. It is a long paper and contains many references.

Dr Martin also suggested looking in the sources of the SCS software engineering module. I have the notebook; I will look through the course notes for principles.

I asked about the appropriateness of including a plan for extended research at the end of my methodology (1 year, 2 years, 5 years, 10 years). Dr Martin said that a dissertation is a document of record. It should be interesting to read in 5 years, maybe even in 10 years. Be cautious of putting a detailed timeline in your thesis. Okay to hint at it, but if you put in detailed predictions you will have egg on your face in 10 years.

Idea: look at software testing books for test coverage principles, etc.

Next meeting: Thursday at 1400. Reading Group on Wednesday (Shamal is presenting a paper of his and Ivan's).

References

[1] Jonathan Bowen and Victoria Stavridou. Safety critical systems, formal methods and standards. *Software Engineering Journal*, 8(4):189–209, 1993.