File 20080519.1400: Notes from meeting with Dr Martin today:

- 30–40 pages is the right length for the assessors.
- We're here because of a mystery: why did a system that's been in production and active development for more than a decade fail to achieve CC evaluation?
    - 'not fit for purpose'
    - Is it because the UK IT scheme evaluators are so much more picky than. . . ?
    - (although there are historical differences *vis-à-vis* risk management or risk avoidance)
- IV&V, parallel code paths, voting
- textbfThesis Statement!
- It's grown and got new capabilities, but it still has the same high assurance architecture—multiple code paths, no single point of failure, two-man control of functions, and the same Software Development Process.
- Include Z schemas *only* if there's a good reason for it to be there.
- Game out risks and contingencies.
- Also, validate the methodology and show that it's a good methodology
    - Validation in front of a conference
- At the end, have I made a contribution? This is the assessors' own success criteria?
- Appendices:
    1. List of documents
- Future work directions:
    - Don't need to dwell on it.
    - It is constructive to list the things you cannot do.
- Methodology
    1. How to interview and why it's important
    2. Process maturity?
        (a) CMMI
        (b) ISO 9001
            - literature
            - audit reports
- Problem
- Interviews
- Solution
- Testing: how do you show that the proposed solution will work?
- Show that if the present project had followed this process, it would have worked.
- Better yet, show how another project would have worked too.

# References