File 20101215.0400 (GMT): ‘Thus, as a result of inherent complexity, CDSs present a uniquely high risk of failure while at the same time haveing the potential to cause a great deal of damage to national security.’ [1]

Timetable:

- 1999: AEHF (‘must be evaluatable at EAL4’)
- 2004–5: RTG 1.0 (failed to achieve Common Criteria evaluation)
- 2006: Research proposal (‘why did it fail’)
  - This became case study № 1.
- 2007: first blind alley: I thought to encode the CC and DCID 6/3 in Z, then prove things about them. The Single XML Description (SXD), which became the Single Extensible Description without changing the acronym.

  Conclusion: C&A is more complicated than just the CC.
- 2008: ‘Develop a Tool to help accreditors’
  - Digression into history.
- 2009: Tool is not going to work until I understand the underlying problem better.
  - Picked up case study № 2: RM 5.0 CT&E under NIST SP 800-53.

  This was followed by lots more blind alleys, dead-end, depression this time last year.
- 2010: Breakthrough—asymmetric information—great problem, but how to solve it?
  - Next blind alley: try to use the developer’s omniscient position, but the accreditors wouldn’t go for it.
  - They did, however, like the idea of a tool that made the other guy do all the work.
  - Failed experiment: overlapping normal distributions with long skew tails, tried combining them and running a moving average over the distribution to get the residual risk: it totally did not work.
- Risk market idea.
- Physical simulation idea
  - And the results seem to match observations dating all the way back to case study № 3, or zero, or whatever it’s called.

References

[1] Joe Loughry. Unsteady ground: Certification to unstable criteria. In *Proceedings of the Second International Conference on Advances in System Testing and Validation Lifecycle*, Nice, France, 22–27 August 2010.