File 20090518.1228: Possibly useful old stuff rescued from an old draft:

Chapter: Introduction

- Motivation
  - The need for useful Certification and Accreditation (C&A)
  - Who needs it and why
  - The dismal state of affairs at present
  - Way out
- A Brief History of the Project
  - There once was an [unnamed] company and it had a successful product...
    - Communication problem in the first Gulf War
    - Radical (for the time) solution proposed
    - Initial resistance from CIA, NSA, and NRO
      1. Removal of human-in-the-loop was thought to be too risky
      2. Prototype approved, but with requirement for (at the time) an unprecedented level of assurance in development.
      3. With experience, role and capabilities were expanded.
  - The system was used all over the world...
    - Currently running in hundreds of locations worldwide
    - More capabilities now, but the development process (and certification requirements) have remained the same.
    - The world has changed, competitors have appeared, and international certification is now required.
  - Now Fast-Forward to 2006
    - The attempted Common Criteria evaluation was a disaster.
    - The functionality is all there, and the software development process used by the developer is a model of process and procedure.
    - WHAT HAPPENED?
- Summary of Contributions
  - An improved method for shepherding existing systems through Common Criteria evaluation
  - Applicable to EAL4+ and higher evaluation assurance levels
  - Several case studies showing before-and-after examples of work package components, elucidating the criteria used by actual NIAP evaluators (from personal interviews)
  - A new plan for successful evaluations in future.

Chapter: Literature Survey

- History of certification and accreditation processes in U.S. and U.K.
- Common Criteria for Information Technology Security Evaluation
  - National Schemes
    1. U.S. NIAP CCEVS
    2. U.K. IT Security Evaluation and Certification Scheme
    3. Other relevant schemes such as the German *Bundesamt fur Sicherheit in der Informationstechnik*, Canadian CCECS, and the Australian Defence Signals Directorate
  - Other Sources
    - CC-CMTS mailing list archive

        - ∗ Guides to CC evaluation (not so much)
        - ∗ Information available from the certified testing labs

- The literature of project failures
    - The literature of failure is extensive [2, 1].
        - ∗ Project management
        - ∗ IT projects
        - ∗ Engineering projects

- Safety literature
    - Safety Cases
    - Process (chemical) engineering
    - International air transport
    - Nuclear power generation
        1. Civilian
        2. Naval

Chapter: Methodology

- Data Sources
    - Project records (3.2 GB total)
        1. Requirements, plans, schedules, emails, reports, draft and final work packages, subcontractor reports, budgets, diary
    - Interviews with participants
        1. Contractor
            (a) Project managers (turnover—several)
        2. Subcontractor
            (a) Project managers (turnover—many)
            (b) Software developers (turnover—several)
            (c) Technical writers (turnover—several)
            (d) Training developers
            (e) Installers (incl. site survey)
        3. Validation lab (sub-subcontractor)
            (a) Project manager
            (b) Validators (turnover—many)
            (c) Other validators (in re: previous successful evaluations)
        4. U.K. national scheme
            (a) Evaluators
        5. MoD customer
        6. U.S. program office (military)
        7. U.S. originating program certifier
        8. U.S. national scheme
            (a) Evaluators
            (b) Authors of previous evaluation schemes (TCSEC, ITSEC)
        9. IV&V contractor
    - Other CC scheme evaluation experts
        1. CC-CMTS mailing list
        2. Andy Cooper

    3. Seek out other experts on the net

- Legal and Regulatory Compliance
  - Proprietary information agreement in-place
  - Export Control
  - ITAR
  - CUREC (Central University Research Ethics Committee)
  - Classified information
  - Pre-publication Review
    1. U.S. Department of Defense
    2. My employer
  - Anonymisation requirement
- Theoretical Component
  - TBD
  - Plan for successful validation and evaluation
  - Structural differences between the Software Development Process in-place and what is described in the Common Criteria

Chapter: Plan for Implementation

- Research Schedule
  - Month-by-month
  - Overview
- Planned sequence of papers for publication
  - First paper
    1. Topic/title
    2. List of proposed conferences
  - Second paper
    1. Topic/title
    2. List of proposed conferences
  - Third paper
    1. Topic/title
    2. List of proposed conferences
  - Fourth paper
    1. Topic/title
    2. List of proposed conferences
- CM plan
  - Tools
  - Repository
- INFOSEC Plan
  - Safeguarding of proprietary information
  - Backup plan
- Confirmation of Status Report

- Writing Plan
- Research Trips
- List of Deliverables
  - Gantt chart schedule of dates
- Definition of Success Criteria

References

[1] Trevor Kletz. *Still Going Wrong!: Case Histories of Process Plant Disasters and How They Could Have Been Avoided*. Gulf Professional Publishing, Burlington, Massachusetts, 2003.

[2] Trevor A. Kletz. *What Went Wrong?: Case Histories of Process Plant Disasters*. Elsevier, Burlington, Massachusetts, fourth edition, 1999.