Vulnerabilities, Vulnerabilities, Vulnerabilities

Simon Milford

LogicaCMG UK Limited – CC Testing Laboratory Manager

With acknowledgements to the work done by:
Steve Hill – LogicaCMG
Tony Boswell – SiVenture

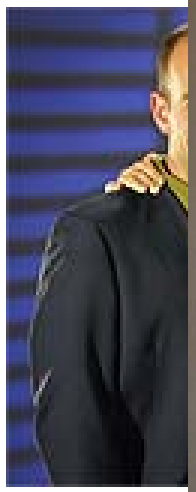
© LogicaCMG 2006. All rights reserved

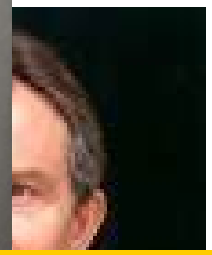
Who am I?

- LogicaCMG Common Criteria Test Lab Manager
- We do:
  - Common Criteria
  - ITSEC
  - UK HMG Schemes (Fast Track, SYS n, Tailored Assurance
  - Central Sponsor for Information Assurance – Claims Tested Mark
  - Cryptographic Module Validation – FIPS 140
- My CV:
  - 12 years at Logica and LogicaCMG
  - 5 ICCCs

What links these people …

The answer ...





n, Location

Vulnerabilities, Vulnerabilities, Vulnerabilities

What is the point of Evaluations …

UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P210

Oracle Internet Directory 10*g*
Release 9.0.4.0.0
running on specified platforms

To get a certificate?

what does the certificate mean, why do we want it, what benefits does it give us?

To improve product development processes?

by having an independent review of how products are developed

To identify product weaknesses before the bad boys do?

do your critical testing in safety, rather than on the Internet

How do we do Evaluations …

Start with a ST

Move through design specifications (FS/HLD/LLD …)

Review testing

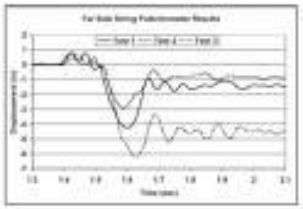
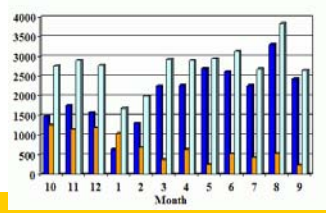


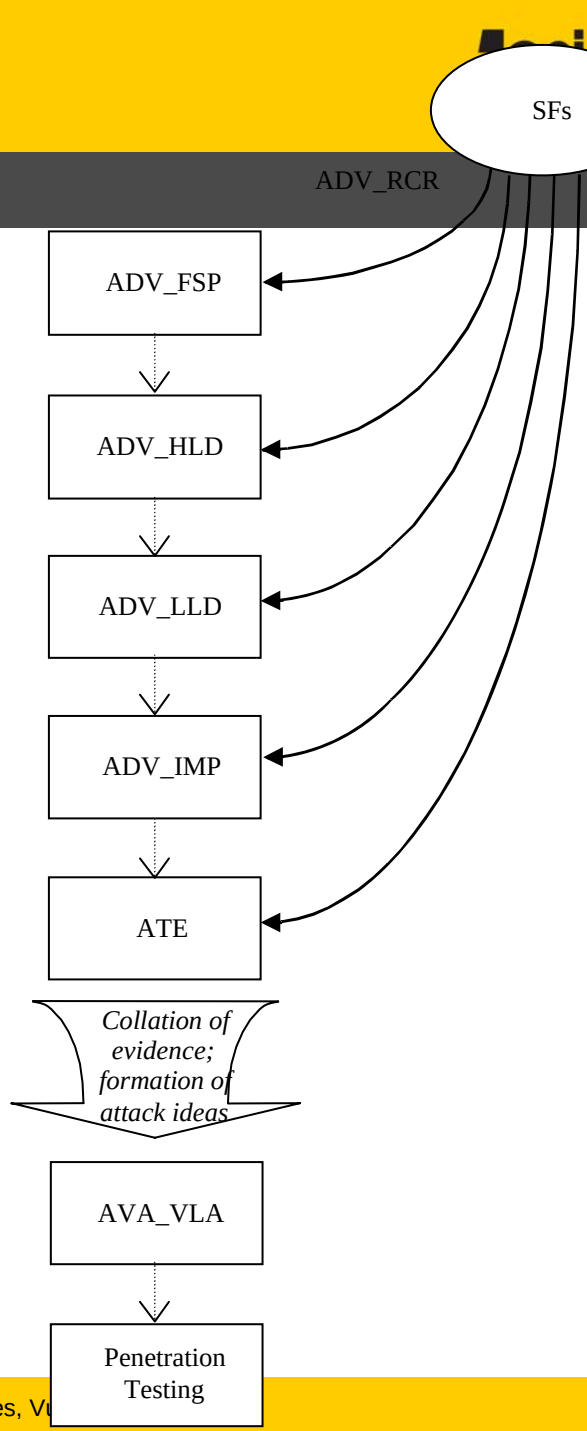
Figure 16. Driver's (Far) side string potentiometer data.

Independent testing

Reporting



How we do Evaluations (2)



Why Do We Work Sequentially

- Because CC is written that way!
  - looks as though that is the way evaluations are intended to be run
- Work Items are expressed linearly
- Reporting is expressed in terms of work items
- Therefore – most efficient and least risky way of working “must” be linear

Time Available for work units …

Work Unit

ST

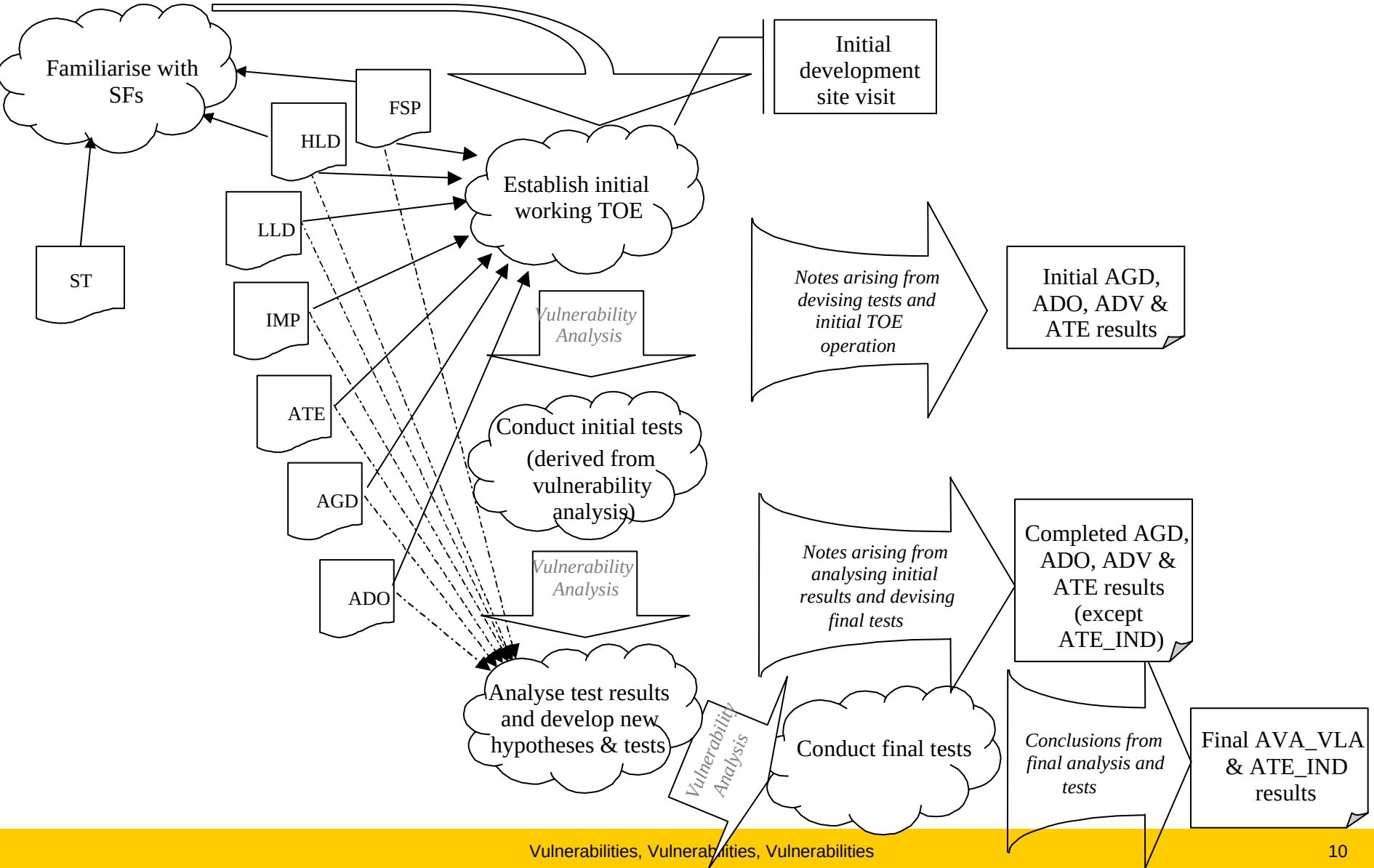
FS/HLD/LLD …

Review testing

Independent testing

Time pressure

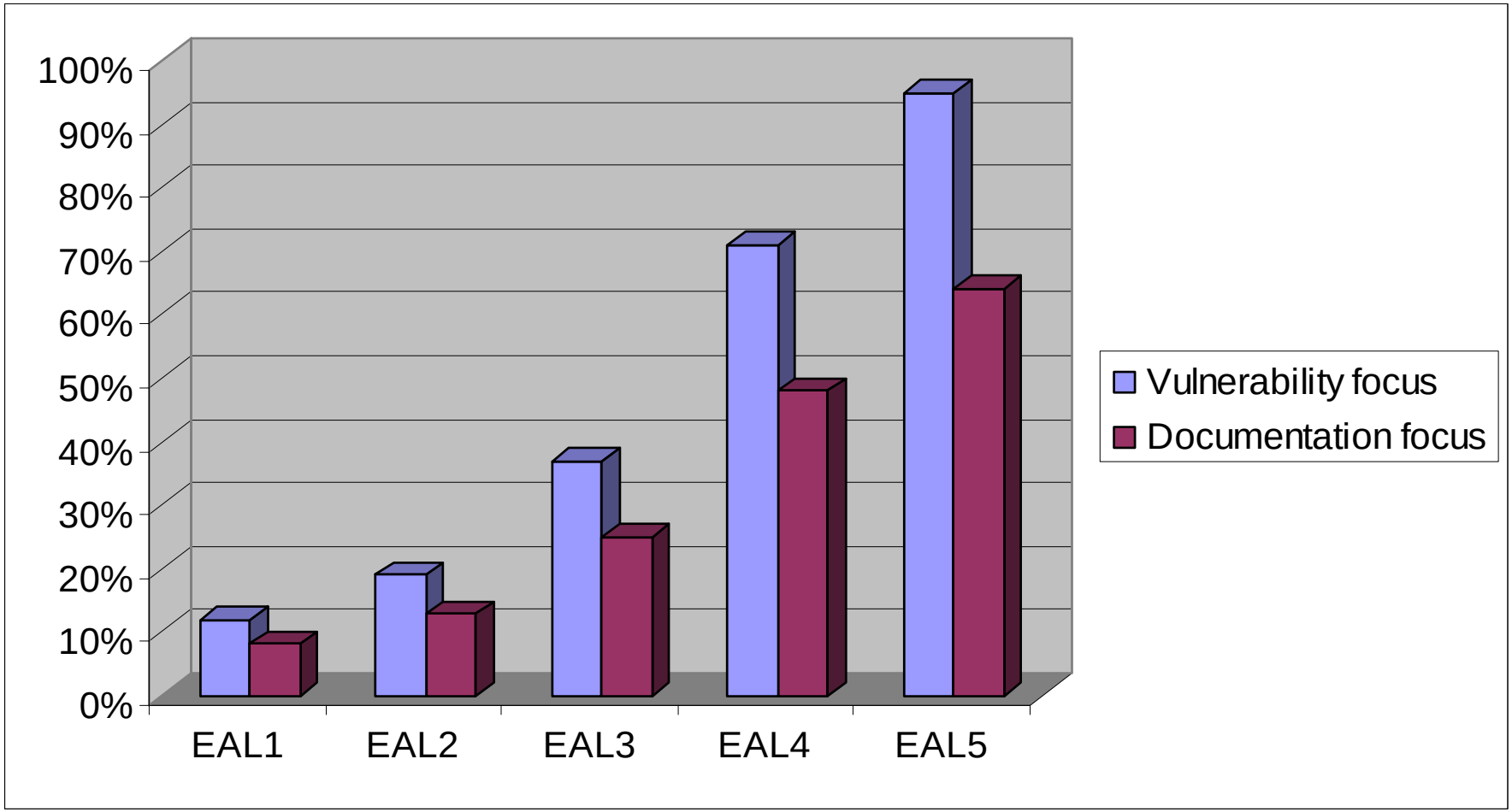
An Alternative Approach



What Are Major Differences

- Construct an operational TOE early on
- Early visit to the Developer – to develop better understanding of the TOE, and the design an doperation of the SFs
- Conduct early set of penetration and functional tests
- BUT – still all based on CC/CEM defined work units

What is impact on Vulnerability Detection?



From a Waterfall to a Fountain …

Barcelona - Fountains at Plaza España