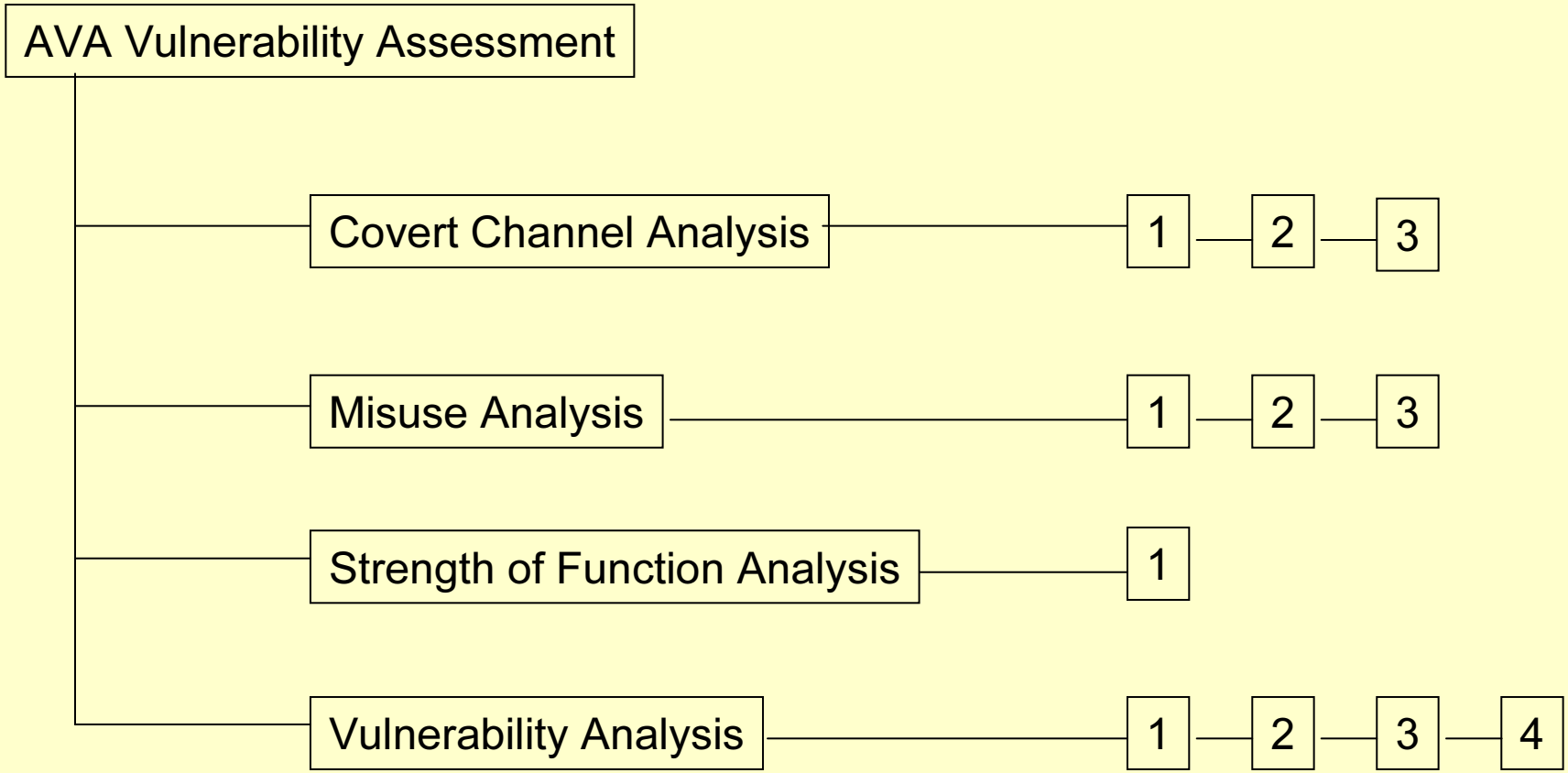
Common Criteria

AVA updates in v3.0

David Martin CESG UK

Common Criteria

AVA Class in v2.x



AVA_CCA Covert Channel Analysis

- Illicit information flows
- Only applicable to certain TOEs
- Included in EAL5
- Many papers written about how to complete such an analysis
- A specific type of vulnerability that can be considered in vulnerability analysis

Common Criteria

AVA_SOF Strength of Function Analysis

- Analysis of particular group of (probabilistic/permutational) mechanisms that have inherent weakness
  - Can be broken through brute-force attack
- Should be consistent with attack potential
- Included in every EAL, but not applicable to every TOE
- A specific example of "direct attack" considered in vulnerability analysis

Common Criteria

AVA_MSU Misuse Analysis

- Part of it is the “reasonableness” of the guidance documentation analysis (AGD)
- Only included at EAL3 and above
- Ways to “mis-use” the TOE is an aspect of vulnerability analysis

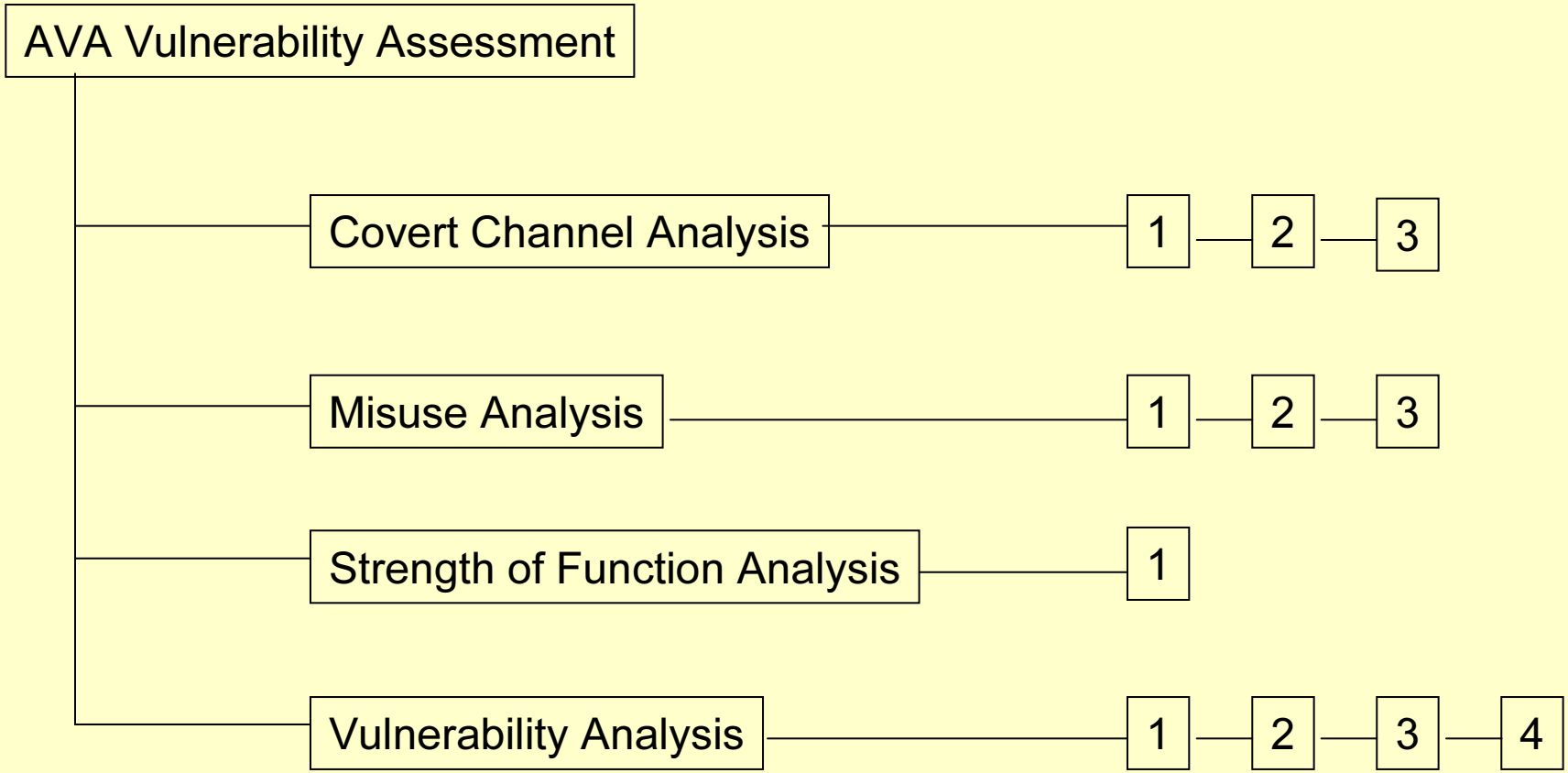
Common Criteria

AVA_VLA Vulnerability Analysis

- No vulnerability analysis at EAL1
  - Although majority of schemes mandated some form of analysis was performed
  - A catch-all in ATE_IND.2
- Unbalanced level of assurance at EAL4

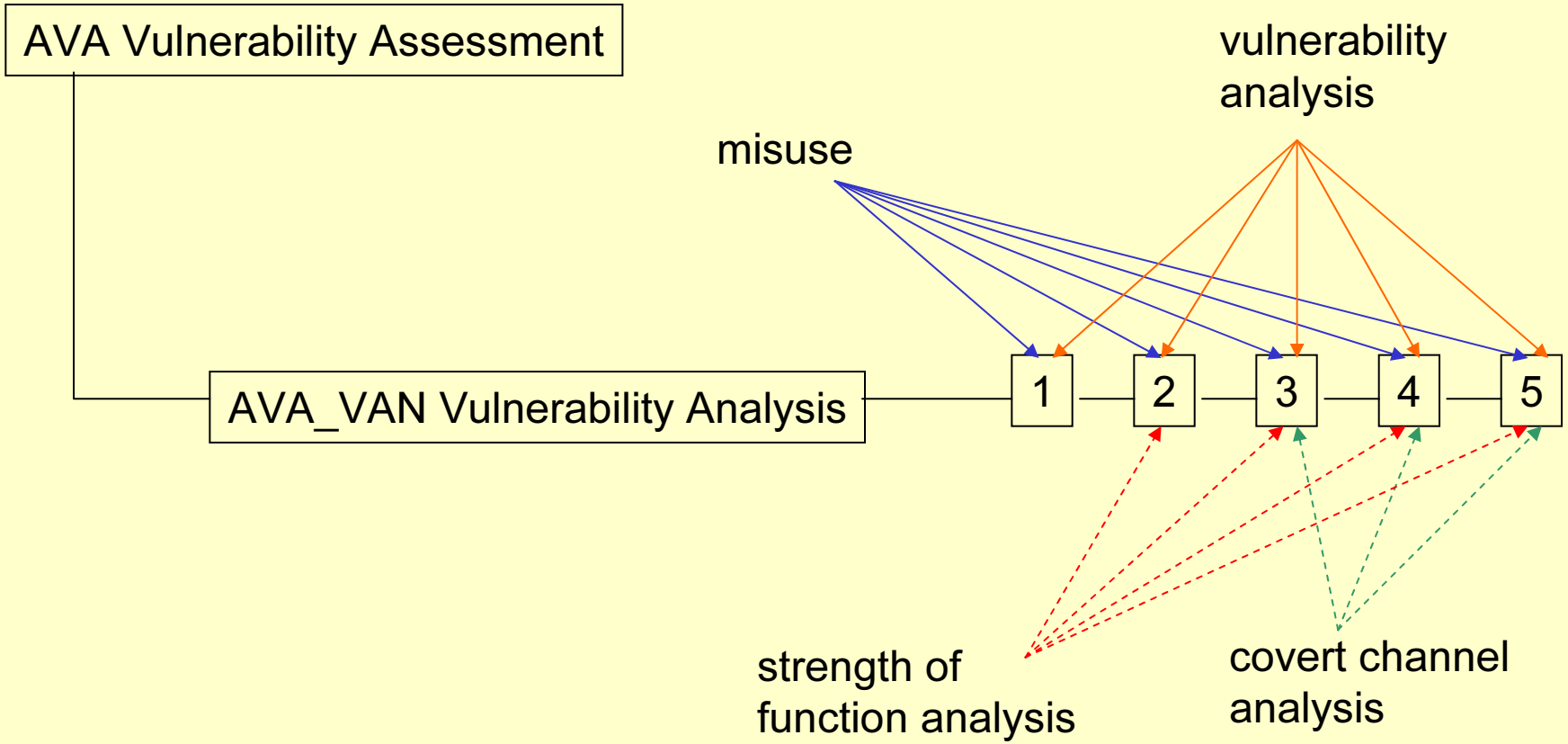
Common Criteria

AVA Class in v2.x



Common Criteria

AVA Class in v3.0



Common Criteria

Family structure

- Levelled on:
  - Inputs: evaluation evidence used in the analysis
  - Rigour
    - of the analysis
    - of the testing performed (attack potential applied in penetration testing)

Common Criteria

AVA_VAN.1 Vulnerability Survey

- Search of public domain sources, e.g.
  - Mailing lists
  - Vulnerability websites
- Encountered vulnerabilities:
  - Identified during conduct of non-AVA evaluation activities.
  - No activity analysis of evaluation evidence for vulnerabilities
- Penetration testing of items identified applying Basic attack potential

Common Criteria

AVA_VAN.2 Vulnerability Analysis

- Active analysis of the TOE by the evaluators using:
  - guidance docs
  - functional specification
  - TOE design
- Approach to analysis undefined prior to execution
- Basic attack potential assumed

Common Criteria

AVA_VAN.3 Focused Vulnerability Analysis

- "Focused" analysis of the TOE by the evaluators
  - Return to "areas of concern" identified in ADV
  - Complex aspects of design
  - Reliance for separation
- Inputs include implementation representation
- Extended-basic attack potential assumed

AVA_VAN.4 Methodical Vulnerability Analysis

- Evaluator is to demonstrate the analysis of evidence is “methodical”
  - Structure of analysis is predetermined
    - “ordered and planned approach”
  - What information will be considered
  - How and why information will be considered
- Moderate attack potential assumed

Common Criteria

AVA_VAN.5 Advanced Methodical Vulnerability Analysis

- As for AVA_VAN.5, except HIGH attack potential assumed
- Resources no issue
  - effort, equipment, knowledge, expertise
- Constraining factors:
  - available window of opportunity e.g. before discovery
  - obtaining samples of the TOE in the case of smartcard type technologies

Common Criteria

Summary of changes

- SOF, MSU, CCA all merged with VLA into single family “AVA_VAN”
- No requirements for developer vulnerability analysis
- Introduction of intermediate level of attack potential between Basic and Moderate
  - “Extended Basic”
- Lowest level of vulnerability analysis performed at EAL1