

Jose Emilio Rico
Epoche & Espri
tech@epoche.es



E P O C H E & E S P R I



Effectiveness of evaluations

CC evaluations driven by the Vulnerability Analysis



Common Criteria

Agenda



E P O C H E & E S P R I

- ❑ The VA & The evaluation process
- ❑ VA related activities? All
- ❑ The attack path concept
- ❑ System Evaluation
- ❑ Conclusions



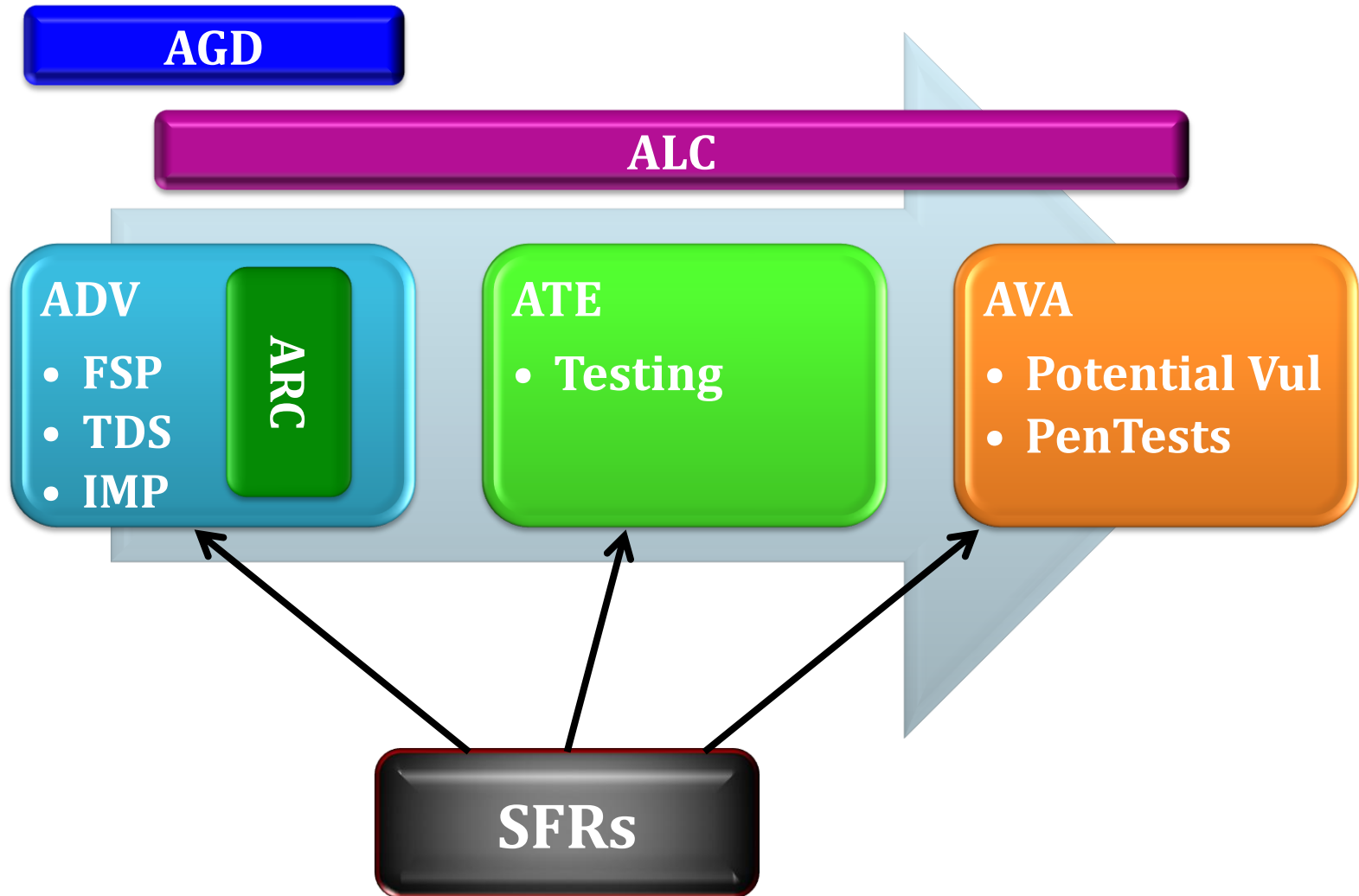
The VA process

- ❑ CC evaluations spend much effort reviewing and correcting the documents to meet content and presentation requirements.
- ❑ This effort could go beyond the usefulness of the documents, which should not be other than to understand the product for conducting the VA.

The VA process



E P O C H E & E S P R I



The VA process



E P O C H E & E S P R I

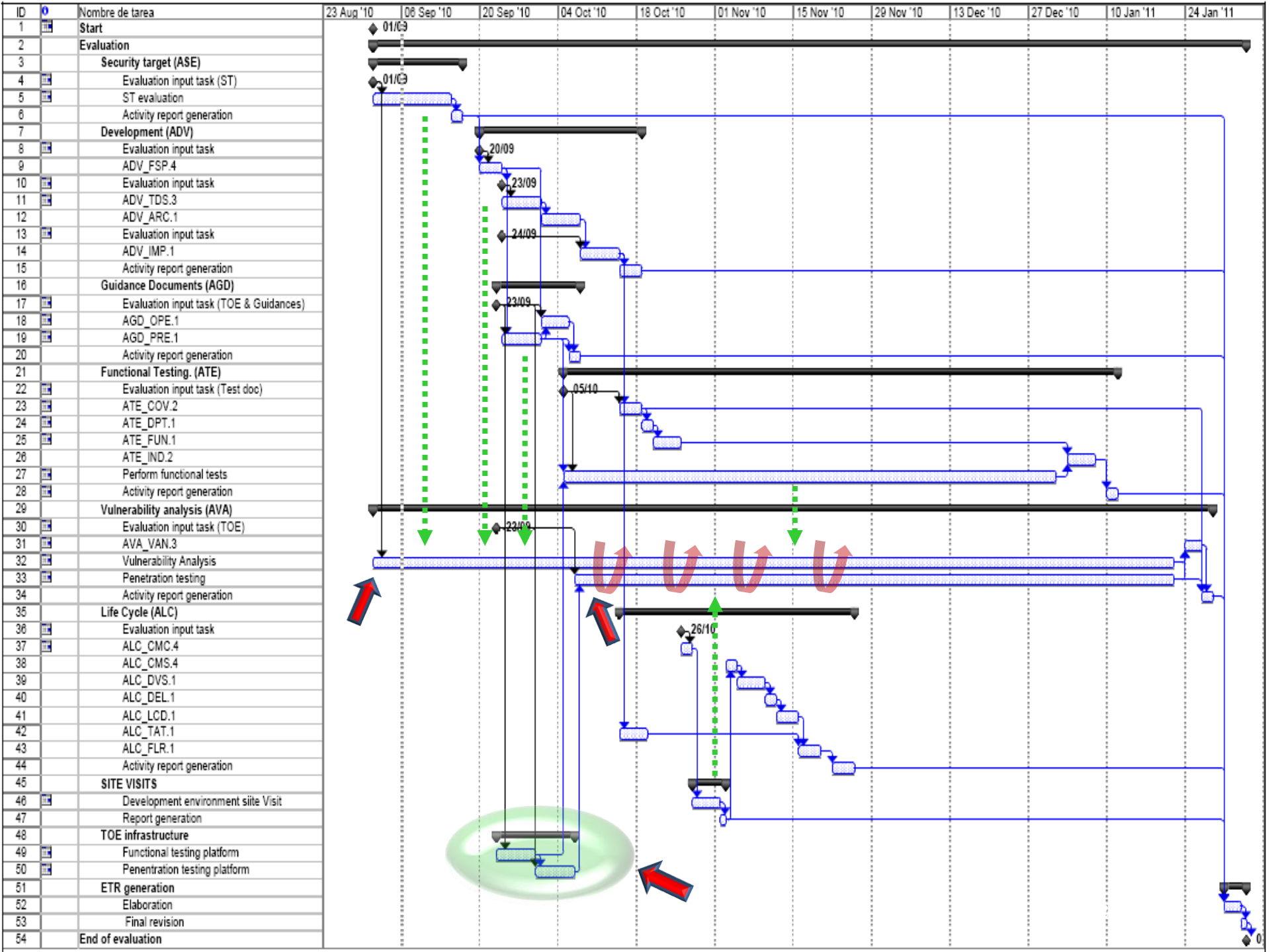
- How should be the VA?
 - An ongoing activity throughout evaluation
 - It should be used to direct every other evaluation activity



The Evaluation process

- How should be the evaluation process?
 - Early analysis of the operation of the TOE
 - Availability of a valid testing platform asap
 - Early set of potential vulnerabilities







1.1 Evaluator action ASE_TSS.1.1E

Verdict	PASS
---------	------

1 The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

1.1.1 Work unit ASE_TSS.1-1

ASE_TSS.1.1C: The TOE summary specification shall describe how the TOE meets each SFR.	
The evaluator <i>shall examine</i> the TOE summary specification to determine that it describes how the TOE meets each SFR.	
Evaluator(s):	
Date:	2010-04-27
Verdict:	PASS

1.1.1.1 References to evaluated evidence

[DS10] Security Target v 1.0, Feb 2010

1.1.1.2 Related Observation Reports and their status

2 xxx-OR-009: CLOSED

1.1.1.3 Work unit summary of findings

3 The section 8 TOE Summary Specification in [DS10], describes how the TOE meets each SFR

1.1.1.4 Work unit verdict and rationale

4 The section 8 TOE Summary Specification

1.1.1.5 Vulnerability analysis notes

5 ASE-VUL-001:

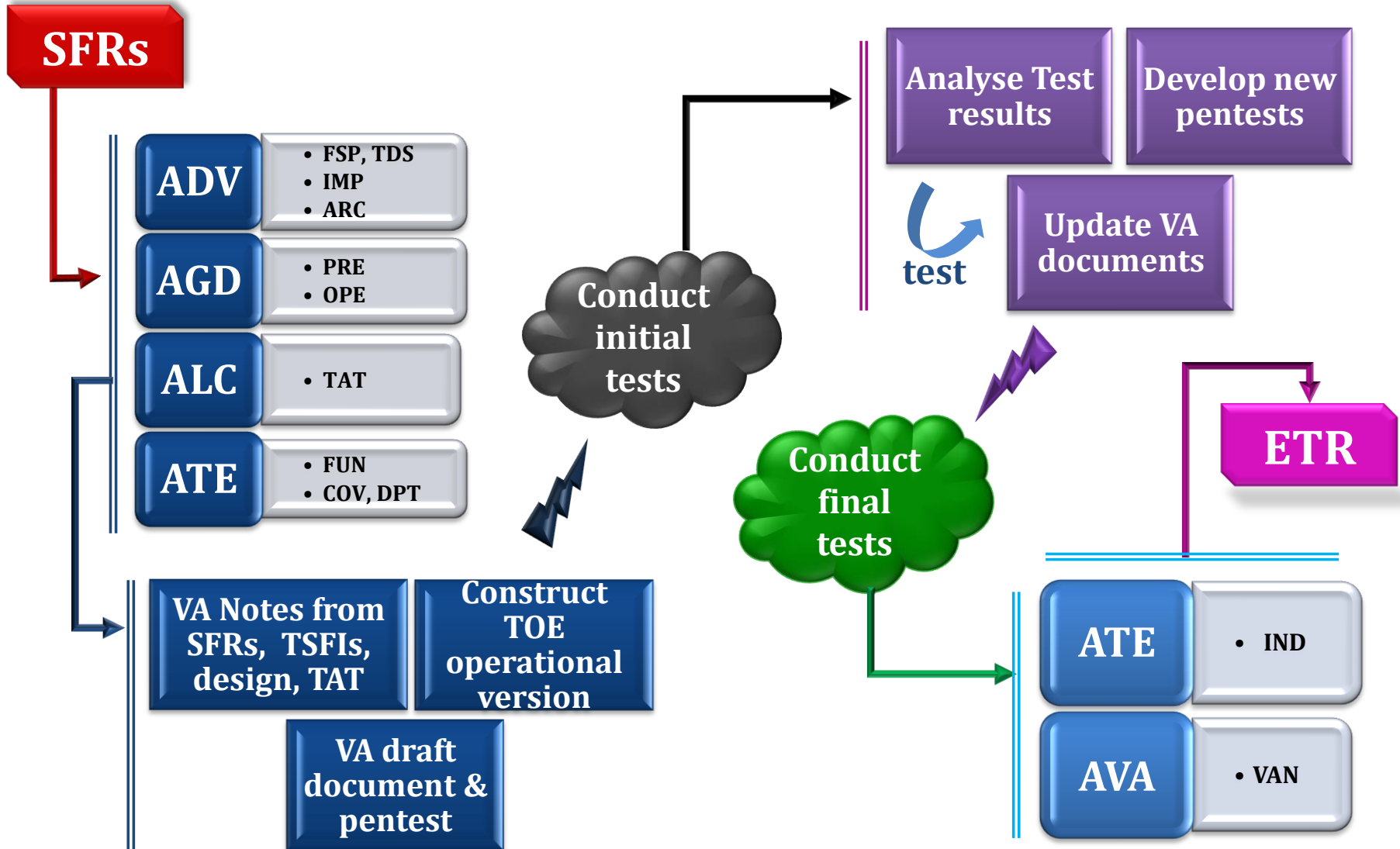
Check the authentication mechanism



The Evaluation process



E P O C H E & E S P R I



VA related activities? All

☐ ASE. Comprehension of the SFRs

- Security Problem resolved
- How the SFRs are represented in the design
- Security Architecture: bypassing or tampering the SFRs.
- How to test the SFRs

VA related activities? All

❑ **Perform evaluation of AGD, ADV, ALC, analyse the developer test documentation (ATE).**

○ **AGD**

Early readiness of a suitable operational platform for testing – AGD_PRE.

Use of prototypes, simulators or emulators.

Misuse or incorrect configuration.

VA related activities? All

❑ Perform evaluation of ADV, AGD, ALC, analyse the developer test documentation (ATE).

- **ADV**

FSP. Penetration tests involves TSFIs.

Subsystems and modules design: temporal or permanent data storage, shared resources.

Exploitation of implementation details

Security architecture



VA related activities? All

❑ Perform evaluation of ADV, AGD, ALC, analyse the developer test documentation (ATE).

○ **ALC** - Development process

CM, DEL, DVS..... Confidentiality & Integrity

TAT. Study the use of problematic constructions allowed by the programming languages.

VA related activities? All

❑ Perform evaluation of ADV, AGD, ALC, analyse the developer test documentation (ATE).

○ **ATE.** Analyse developer documentation

Repeat early some developer tests (ATE_IND)

Carry out additional evaluator functional tests (ATE_IND)

Support the definition of the initial penetration tests (AVA_VAN)

VA related activities? All

Conduct initial Tests.

The penetration test plan and description shall be executed in the testing platform.

In the course of defining and planning the tests, ADV and ATE (except IND) will be completed.

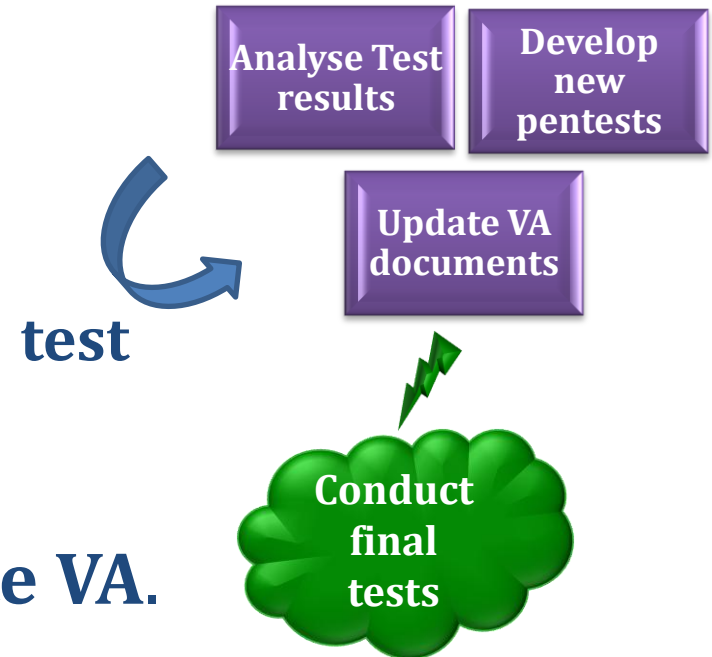
Testing is expected to start early before the completion of ADV and ATE activities.



E P O C H E & E S P R I

VA related activities? All

**Iterative nature of
the penetration testing**



- ❑ **Analyse results and update VA.**

The analysis of initial test results will suggest new tests.

- ❑ **Conduct final Tests.** Stage where IND and Pen testing are finalised. VA completed.

VA related activities? All

❑ Finalise ATE_IND and AVA_VAN.

Update the VA documents with the definitive findings and rationale.

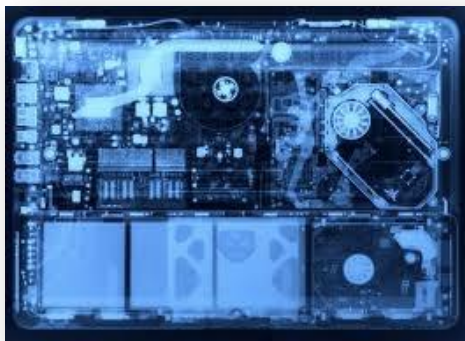
Complete the ATE_IND and AVA_VAN activities.

The final conclusions will be detailed in the ETR, including the VA tasks carried out in each of the CC activities.

The attack path concept

1st - order vulnerabilities

- ❑ Soon confirmed → “*Conduct initial tests*”
- ❑ Do not compromise any particular asset
- ❑ Open the way to compromise the assets through 2nd order exploits



The attack path concept

2nd - order vulnerabilities

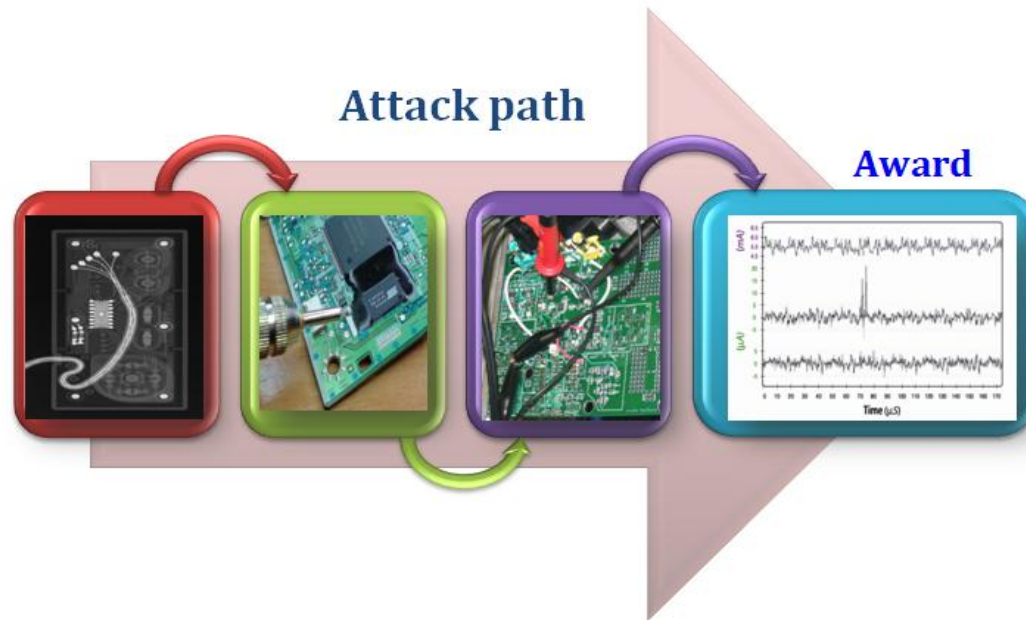
- ❑ Pentests designed from the 1st order results and a deeper knowledge of the TOE internals.
- ❑ The success of the 1st becomes a precondition when designing 2nd-order pentest
- ❑ Compromise an asset
- ❑ Result of the cycle
“Test – Analyse – Design new tests”



The attack path concept



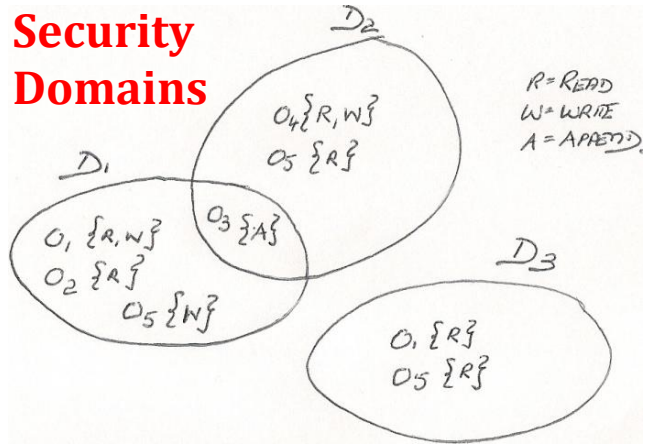
The vulnerability is defined by its full attack path. The process involves several CC activities.



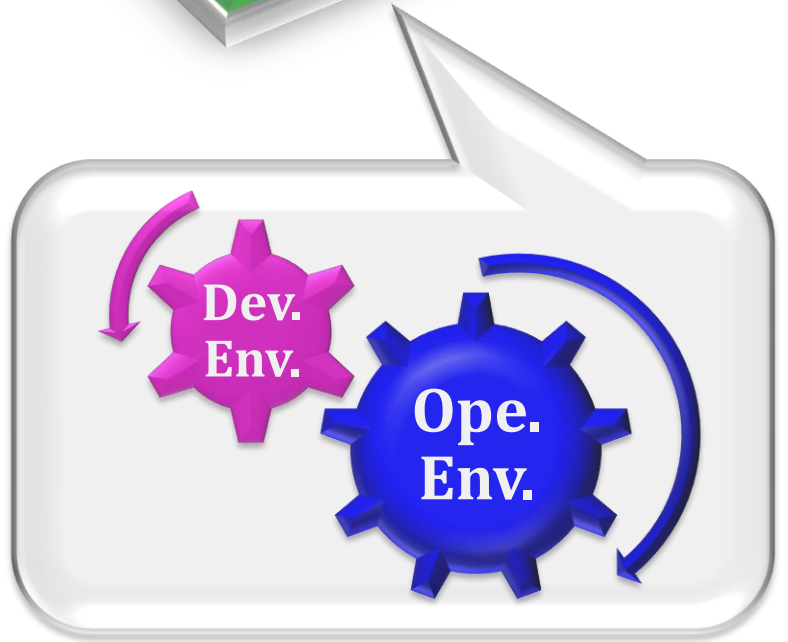
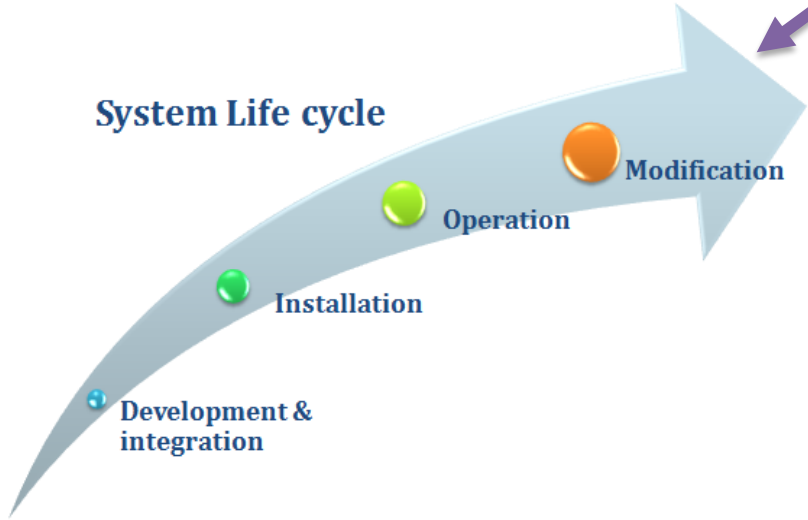
- ❑ X-ray + epoxy encapsulation + probe a bus
- ❑ Overflows + defence in depth + shell-code



Security Domains






System Life cycle



Conclusions

The Vulnerability Analysis is the product of our evaluation model

-  Finding vulnerabilities is the way for improving the security.
-  The VA starts at an early stage, is an ongoing activity throughout evaluation and direct the other CC activities.
-  The approach is applicable to systems evaluations.



E P O C H E & E S P R I



Jose Emilio Rico
tech@epoche.es

Epoche & Espri, S.L.
Avda. de la Vega, 1
28108, Alcobendas, Madrid
Spain

Tel: +34 914-902-900
FAX: +34 916-625-344

Epoche & Espri Corporation
4000 Legato Road, Suite 1100
Fairfax, VA 22033
USA

Tel: +1 888-877-9506
FAX: +1 703-227-7189