Jose Francisco Ruiz Gualda
Epoche & Espri
eval@epoche.es

EPOCHE & ESPRI

Lower EALs evaluations

Are you kidding me?

Common Criteria

Agenda

EPOCHE & ESPRI

- Testing Requirement for EAL
- Non observable SFRs Problem
- Dealing with the problems
- Conclusions

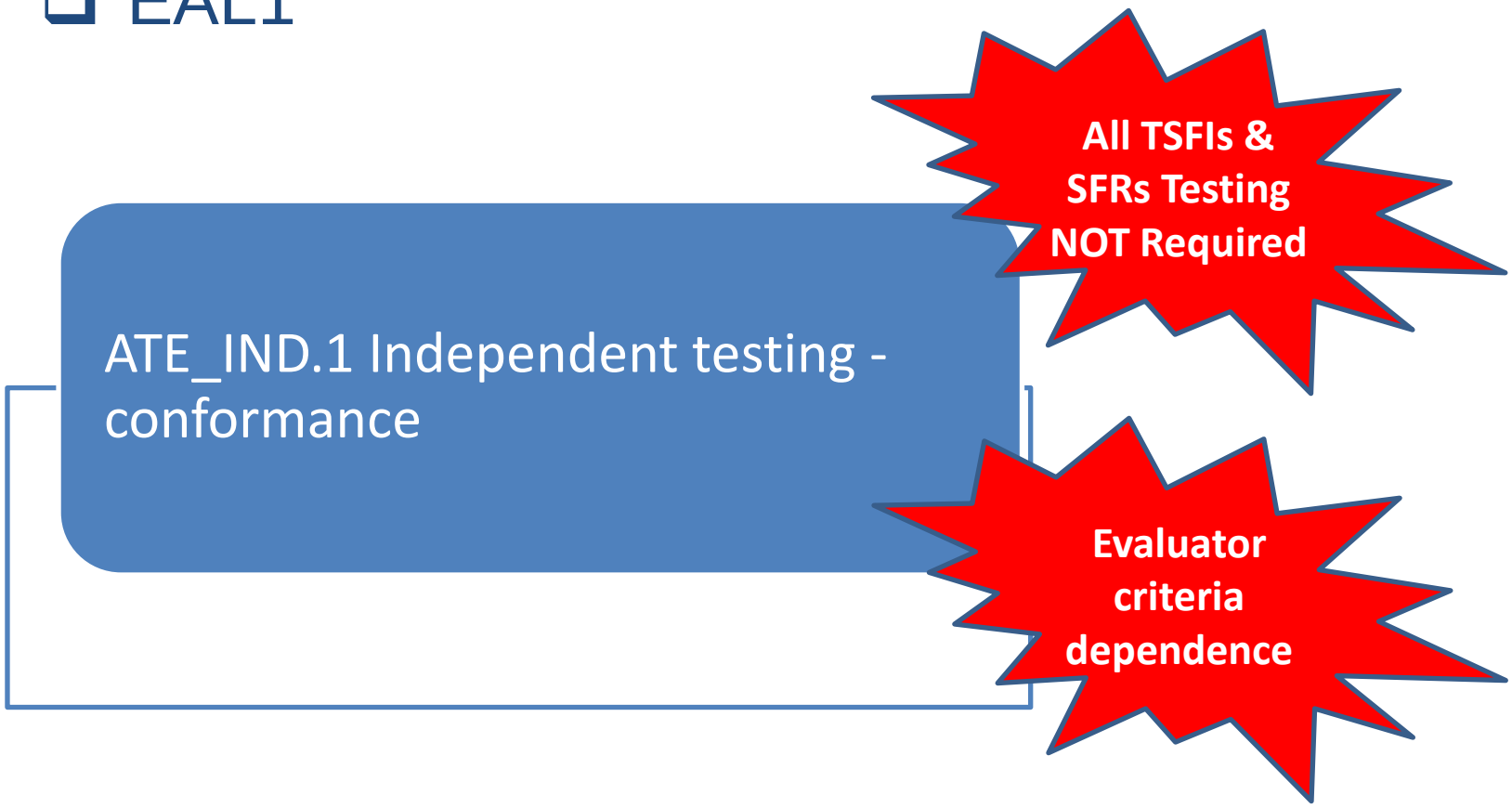
EPOCHE & ESPRI

Testing Requirement for EAL

Testing Requirement for EAL

EPOCHE & ESPRI

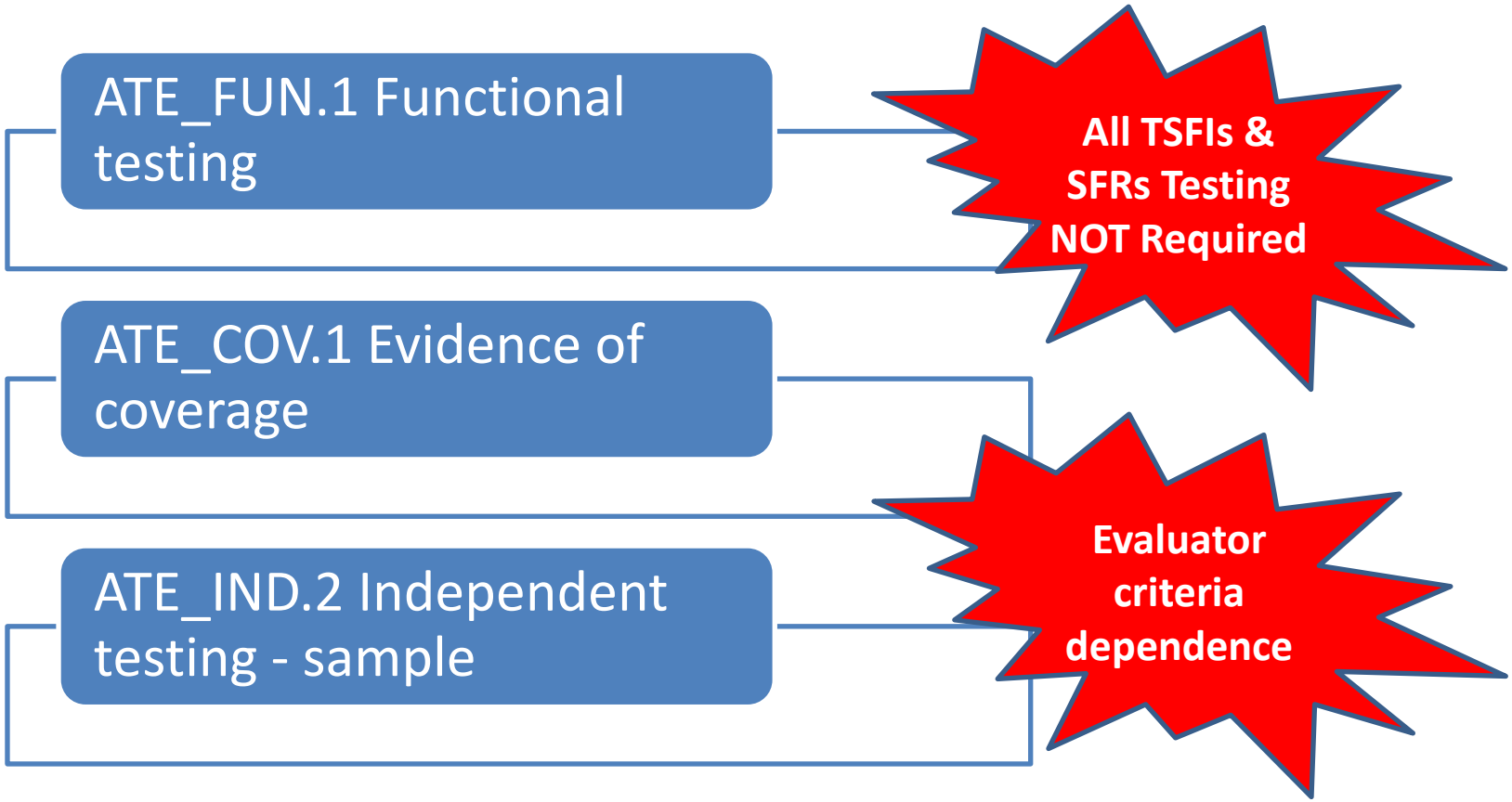
- EAL1



Testing Requirement for EAL

EPOCHE & ESPRI

- EAL2



Testing Requirement for EAL

EPOCHE & ESPRI

- EAL2

"The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF".

Testing Requirement for EAL

EPOCHE & ESPRI

- EAL3 & EAL4

- ATE_COV.2 Analysis of coverage
- ATE_DPT.1 Testing: basic design
- ATE_FUN.1 Functional testing
- ATE_IND.2 Independent testing - sample

All TSFIs & Subsystems & SFRs tested!!

EPOCHE & ESPRI

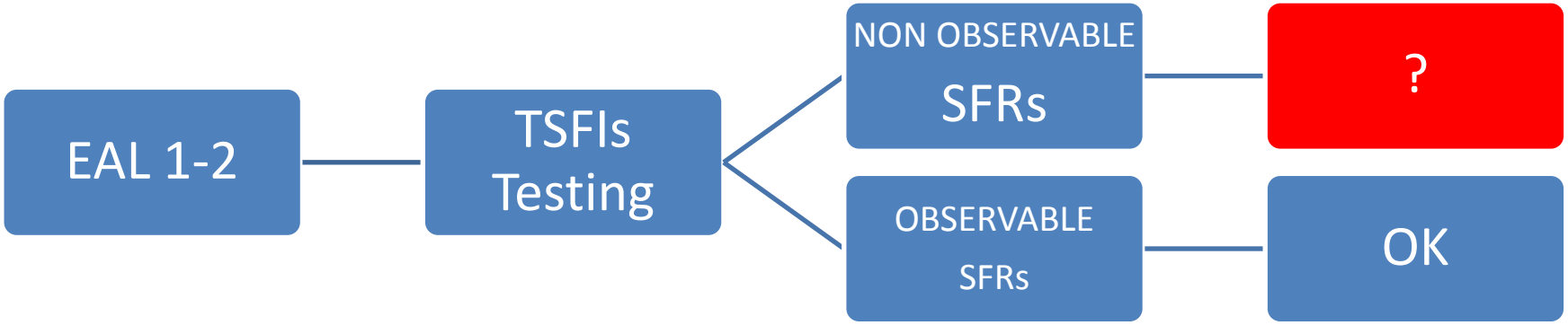
Non observable SFRs Problem

Non observable SFRs Problem

EPOCHE & ESPRI

- Examples of SFRs that could not be externally observable:
  - FDP_RIP: Residual information protection
  - FCS_COP: Cryptographic Operations
  - FDP_SDI: Stored data integrity
  - FAU_STG: Protected audit trail storage

Non observable SFRs Problem

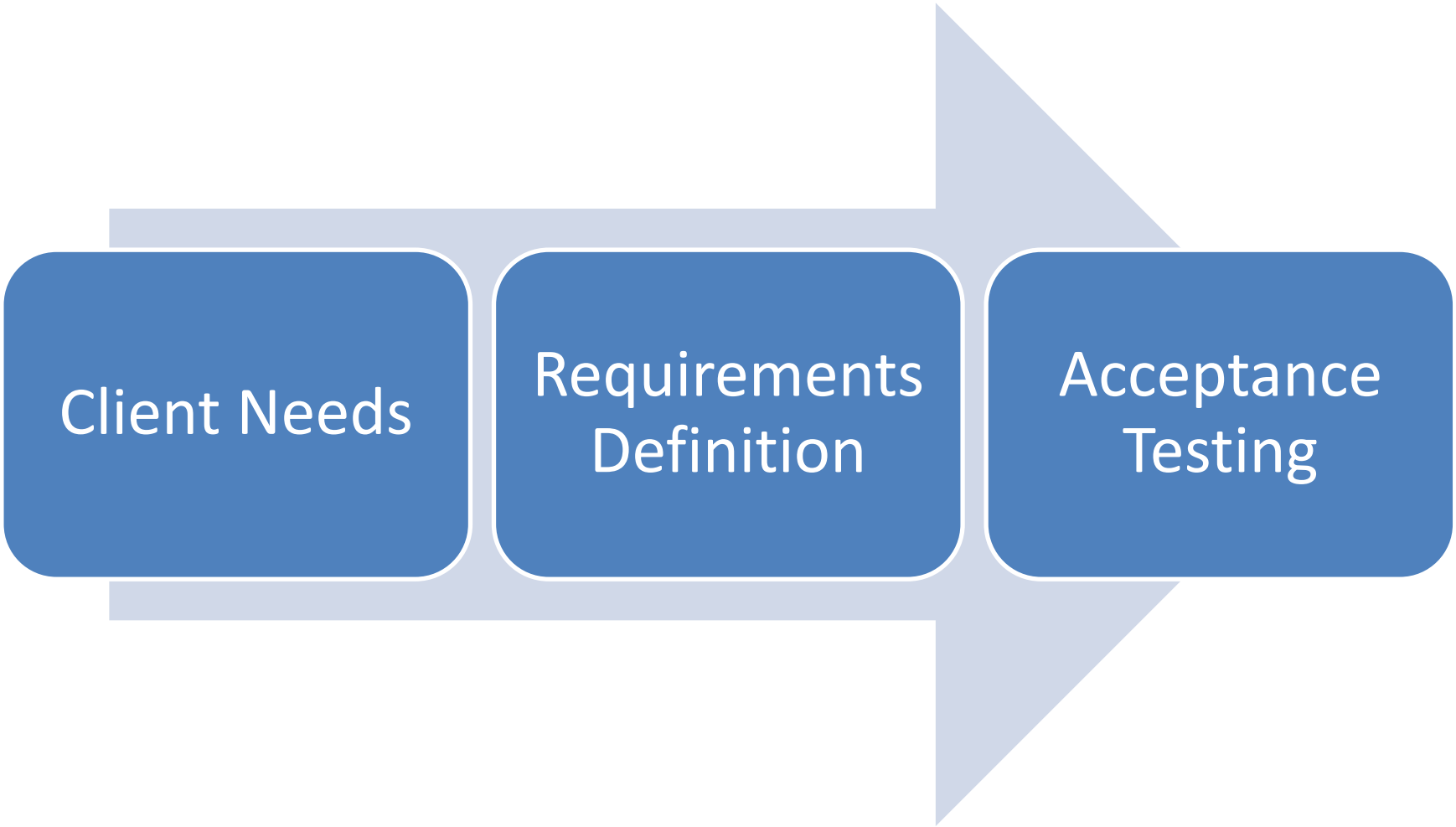


EPOCHE & ESPRI

Dealing with the problems

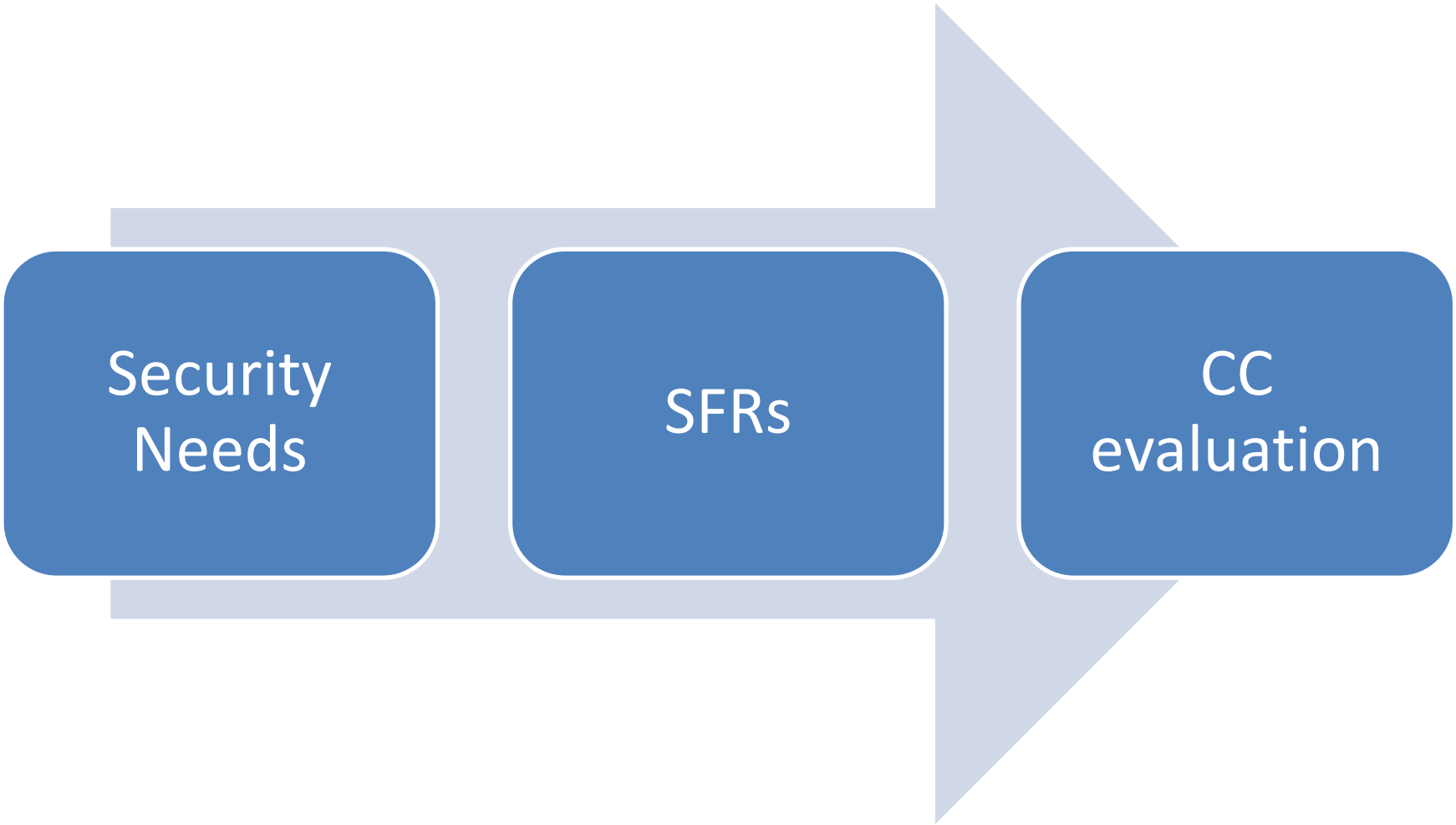
Dealing with the problems

EPOCHE & ESPRI



Dealing with the problems

EPOCHE & ESPRI



Dealing with the problems

EPOCHE & ESPRI

- **Testing Problem: Are ATE activities checking if the TOE fulfills the SFRs?**

Dealing with the problems

EPOCHE & ESPRI

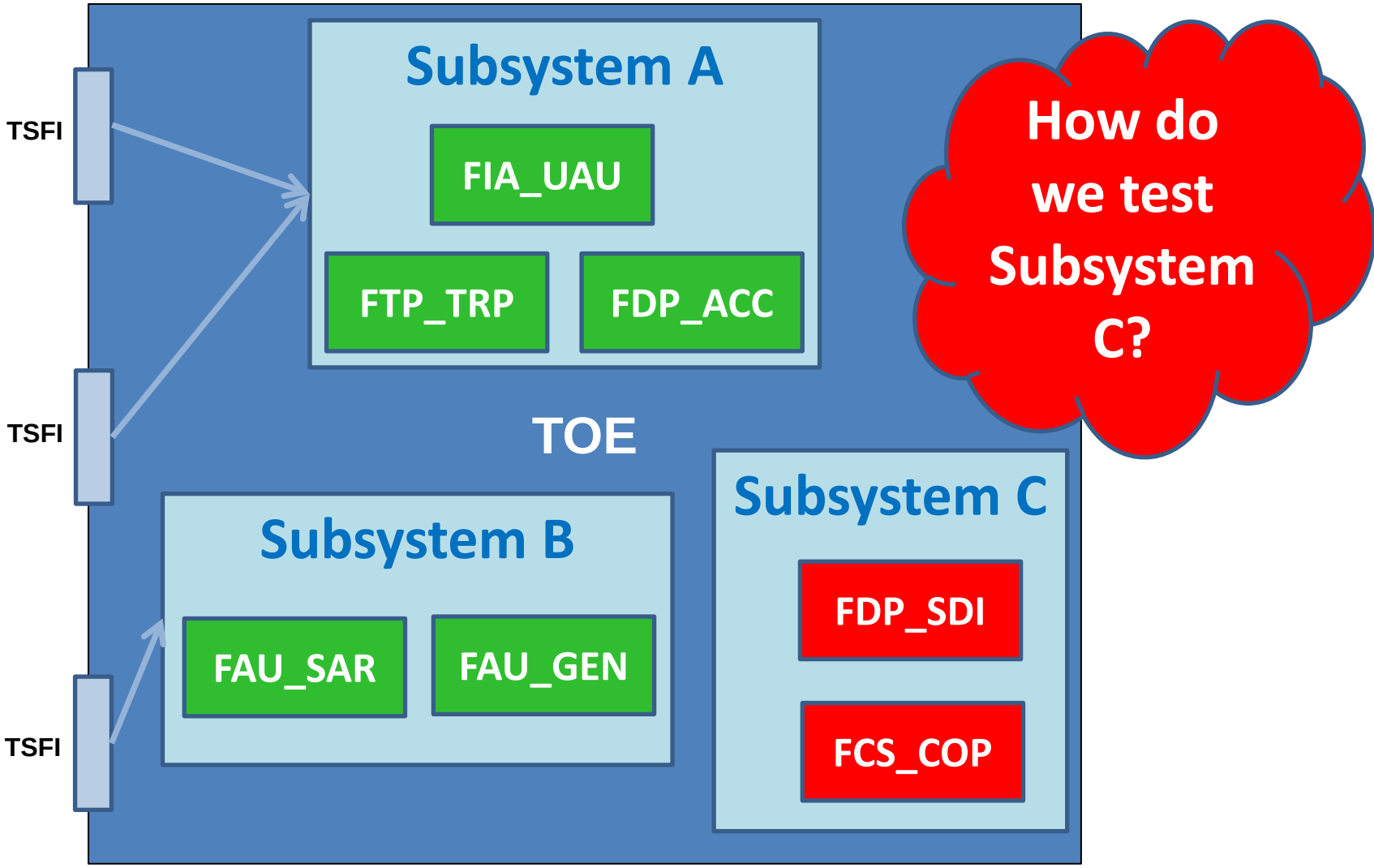
TSFI Testing Approach

- Some SFRs may not be tested

SFR Testing Approach

- All the SFRs are tested
- Lab Effort not commensurate with the required assurance

TSFIs Testing



SFR Testing

EPOCHE & ESPRI

With the developer Support

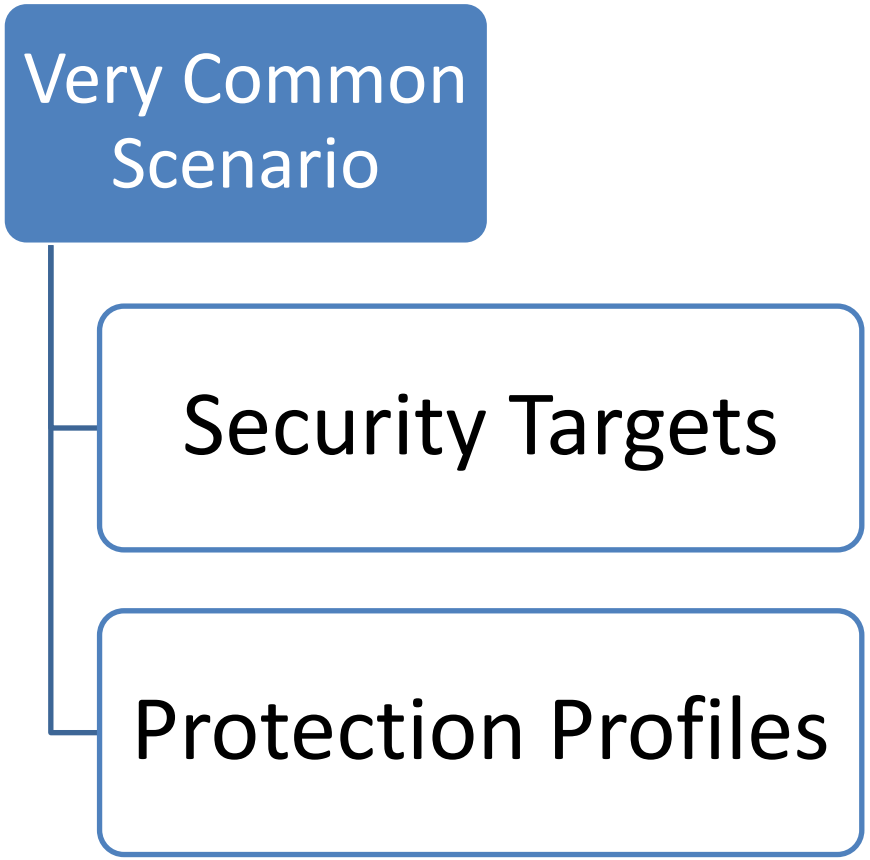
- Guarantee of success
- Additional Testing interfaces
- Debug Specimens
- Source code review

Without the developer Support

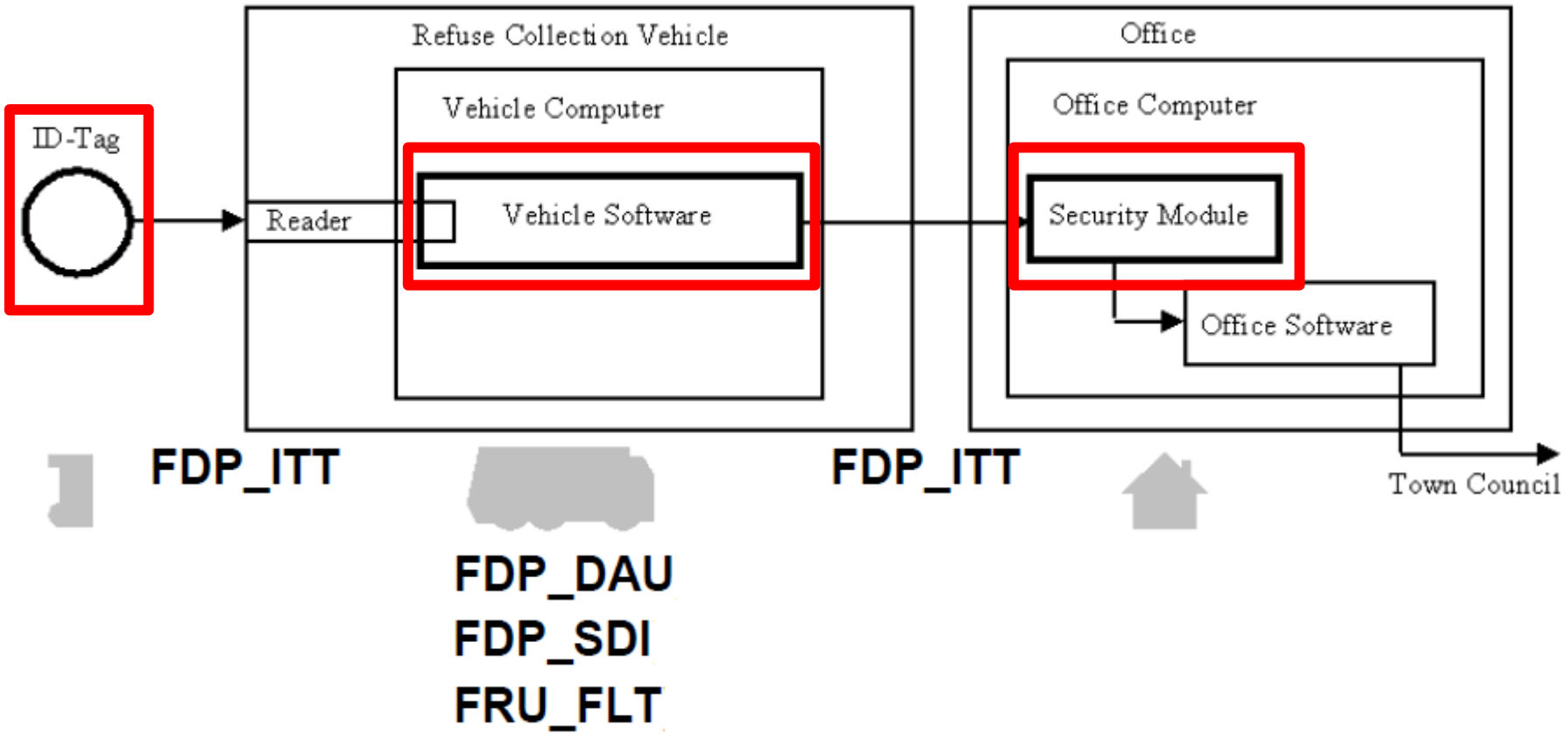
- Reverse Engineering
- Debugging
- Evaluator Magic
- Not Possible?

Common Scenario

EPOCHE & ESPRI

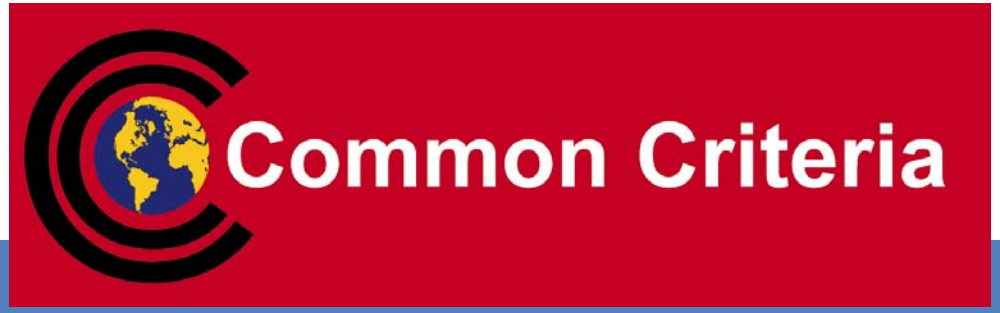


Example: Waste Bin Identification System Protection Profile



SFR Testing: Not Possible?

EPOCHE & ESPRI



Some SFRs not tested

Customer Security needs?

Evaluations Reliability?

Alternatives

EPOCHE & ESPRI

New orientation for ATE activities (IND & COV & DPT)

SFR Testing

- EAL1 (ATE_IND): **SFR testing** through TSFIs + **developer support to test non observable SFRs**
- EAL2: **SFR testing** through TSFIs by the developer (ATE_COV) + **developer support to test non observable SFRs by the evaluator(ATE_IND)** + additional evaluator TSFI testing (ATE_IND)
- EAL3: **SFR testing** through TSFIs/Subsystems by the developer (ATE_COV + ATE_DPT) + additional evaluator testing (ATE_IND)

Alternatives

EPOCHE & ESPRI

Technical Communities

- New Protection Profiles
- SFRs Testing Methodology

Network Devices PP

EPOCHE & ESPRI

FTA_TAB.1.1 **Refinement:** Before establishing **an administrative user** session the TSF shall display **a Security Administrator-specified** advisory **notice and consent** warning message regarding use of the TOE.

Application Note: This requirement is intended to apply to interactive sessions between a human user and a TOE. IT entities establishing connections or programmatic connections (e.g., remote procedure calls over a network) are not required to be covered by this requirement.

Assurance Activity:

The evaluator shall check the TSS to ensure that it details each method of access (local and remote) available to the administrator (e.g., serial port, SSH, HTTPS). The evaluator shall also perform the following test:

Right Approach!!

- Test 1: The evaluator follows the operational guidance to configure a notice and consent warning message. The evaluator shall then, for each method of access specified in the TSS, establish a session with the TOE. The evaluator shall verify that the notice and consent warning message is displayed in each instance.

Network Devices PP

EPOCHE & ESPRI

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] all objects.

Assurance Activity:

"Resources" in the context of this requirement are network packets being sent through (as opposed to "to", as is the case when a security administrator connects to the TOE) the TOE. The concern is that once a network packet is sent, the buffer or memory area used by the packet still contains data from that packet, and that if that buffer is re-used, those data might remain and make their way into a new packet. The evaluator shall check to ensure that the TSS describes packet processing to the extent that they can determine that no data will be reused when processing network packets. The evaluator shall ensure that this description at a minimum describes how the previous data are zeroized/overwritten, and at what point in the buffer processing this occurs.

Wrong Approach!! -> No Test

Alternatives

EPOCHE & ESPRI

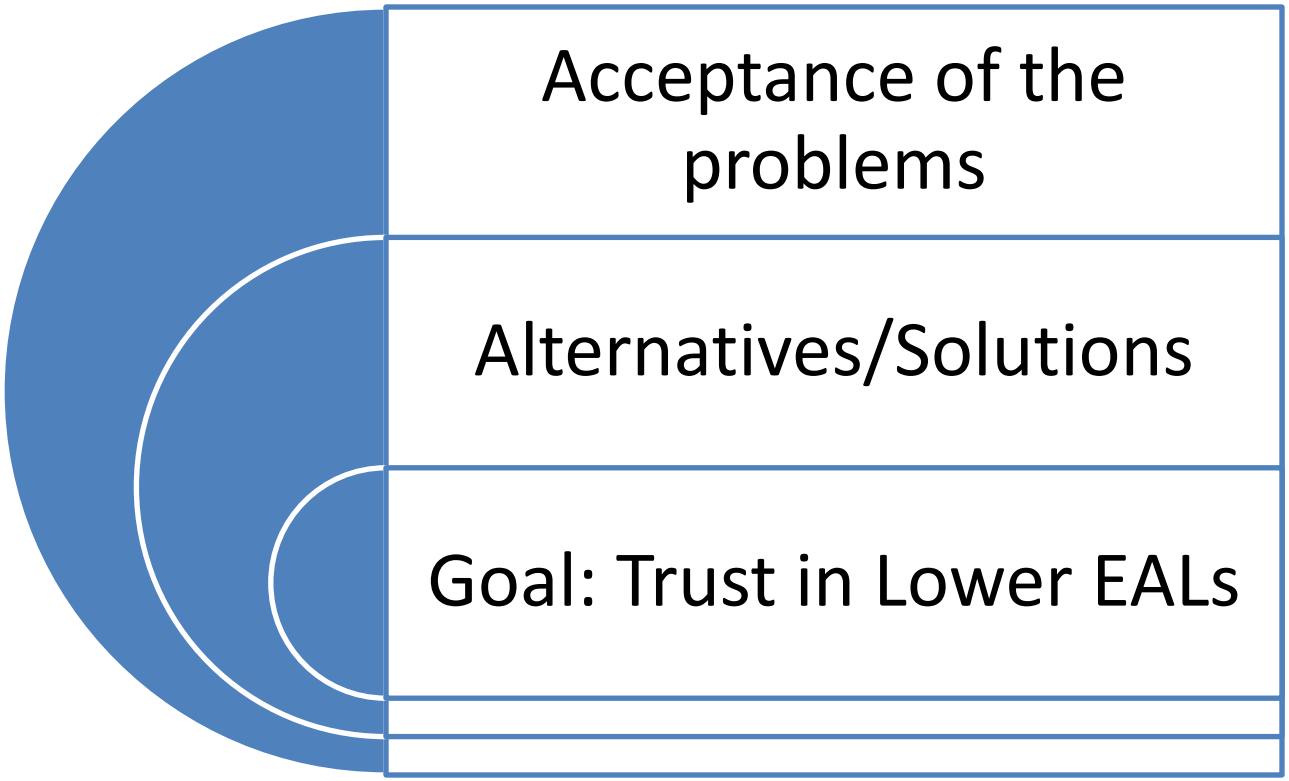
FIPS 140-2 Inspiration

- Flexibility (IG)
- Caveats

Conclusions

Conclusions

EPOCHE & ESPRI



Jose Francisco Ruiz Gualda
eval@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