

ATE evaluation in limited workload

Clément Capel, Oberthur Technologies & Nicolas Lokiec, THALES CEACI
22/09/10 - 11th ICCG, Antalya

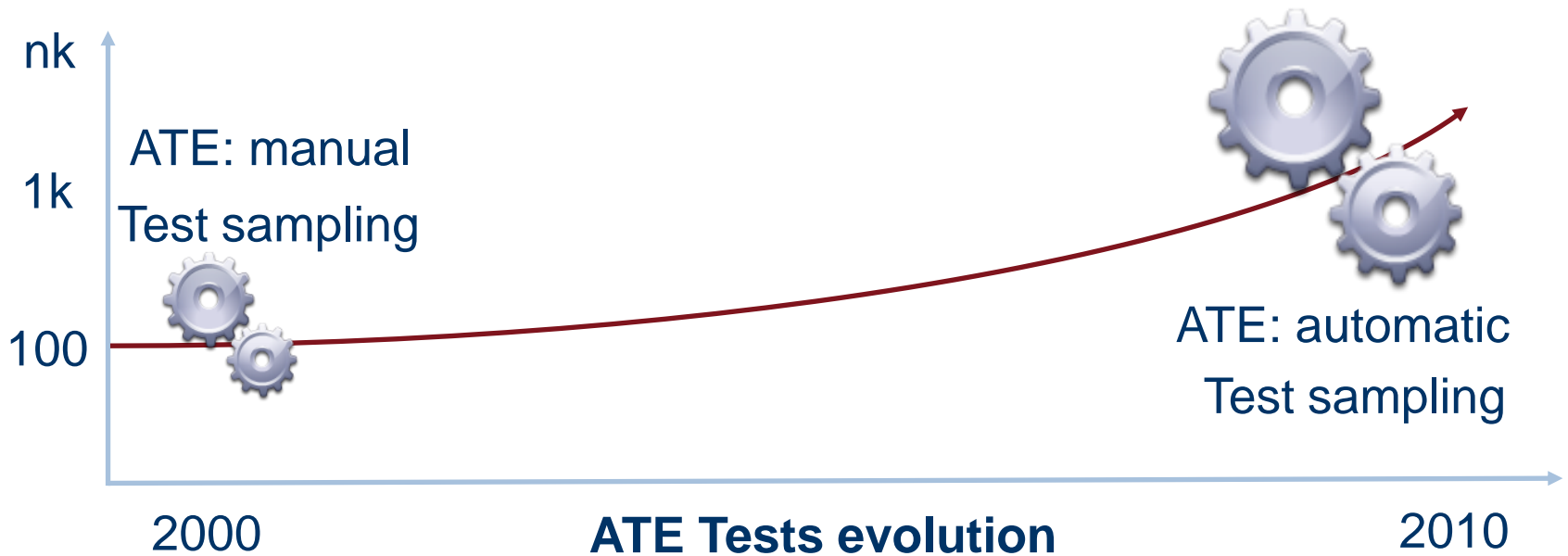


- Evolution of ATE activity and new issues
- New methodology handling boundaries
- The developer is going to organize the testing strategy
- Improvements get from this methodology

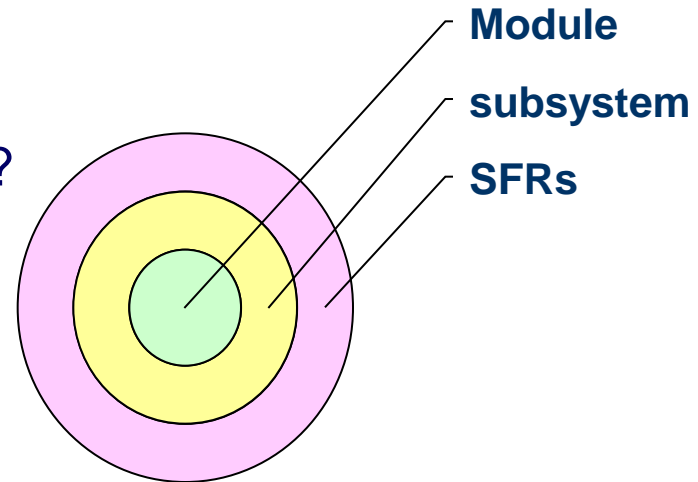


Product evolution regarding ATE

- Code size has increased
- Number of tests has skyrocketed
- Most of tests are now automated
- This is not always balanced



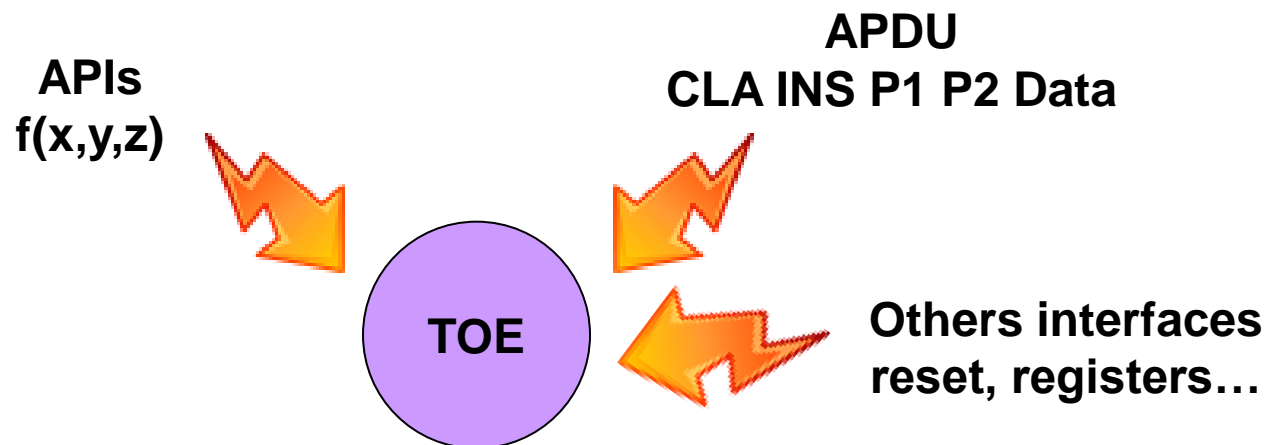
- At first sight, SFRs can cover the full TOE
- All the modules play a role in ATE security
- How performing an efficient test sampling?
- How to be sure TSF is correctly tested?
 - In nominal cases,
 - In error cases
 - In unusual cases.



How the evaluator can ensure that TOE
security features are well tested?

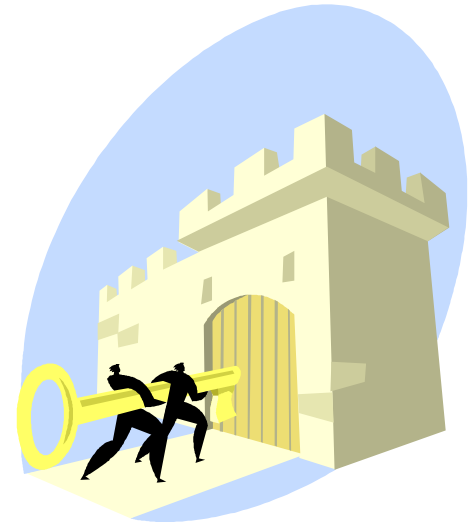


- API and external interfaces are generally stimulated with nominal parameters
- This corresponds to product specification:
 - ePassport,
 - Visa, Mastercard
- Covers part of security aspects



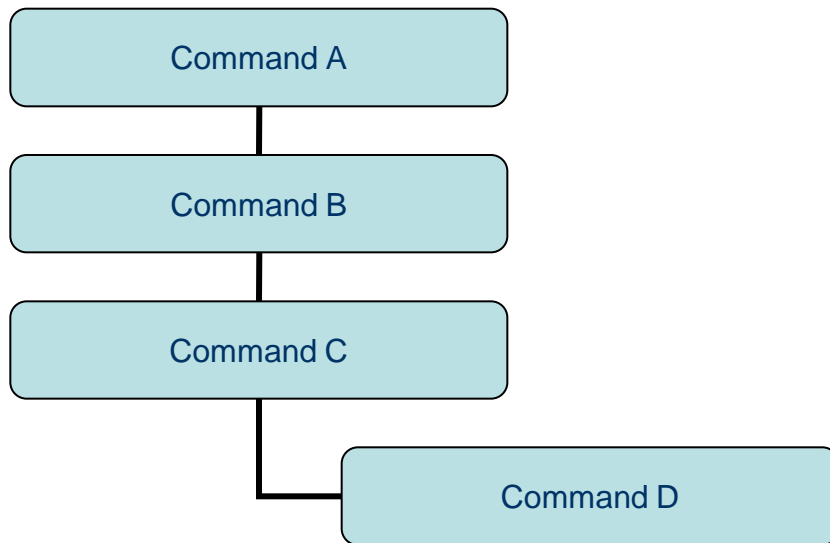
Vulnerability on boundaries

- **How can you be sure that values not tested in nominal cases behave as those expected**
- **If an APDU has a parameter $n \mid n < 0 < 256$ (1byte) ...**
 - What about 0? And 256?
 - Although the APDU should not be stimulated that way...
- **If not correctly managed:**
 - can induce unexpected behavior,
 - reveal unwilled trapdoors.

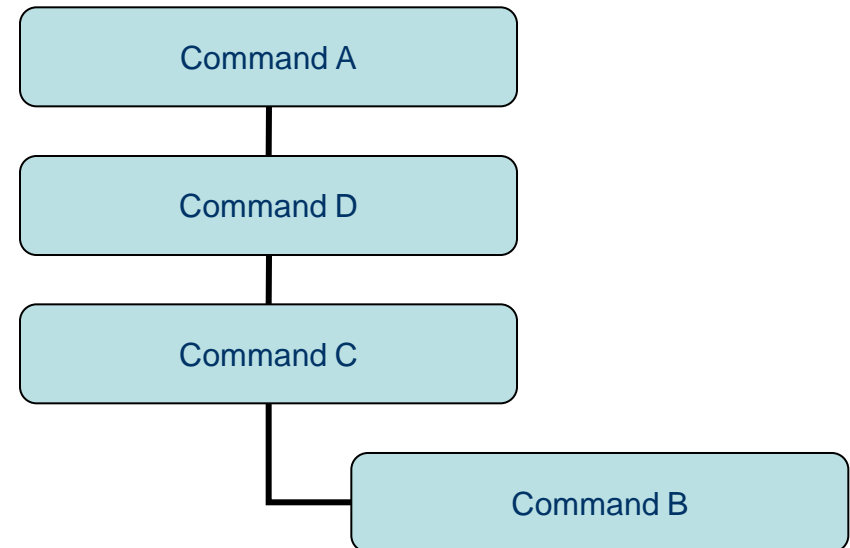


Command flow perturbation

First « nominal »
sequence tested



Second « unusual »
sequence not tested



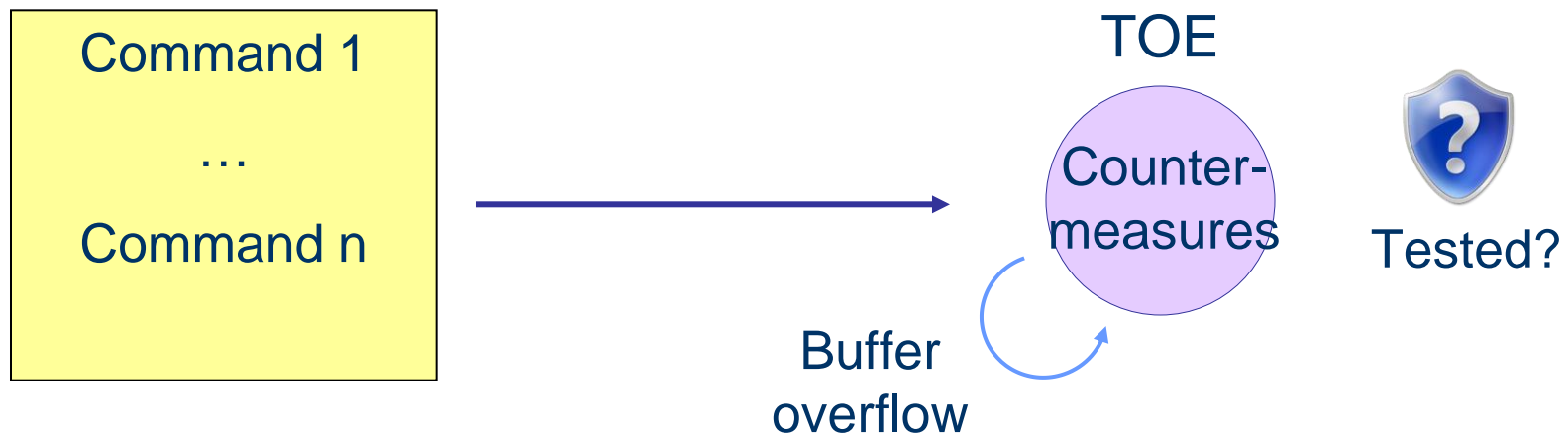
Are the two behaviours equivalent?

Is it reasonable not taking into account the “unusual case”?

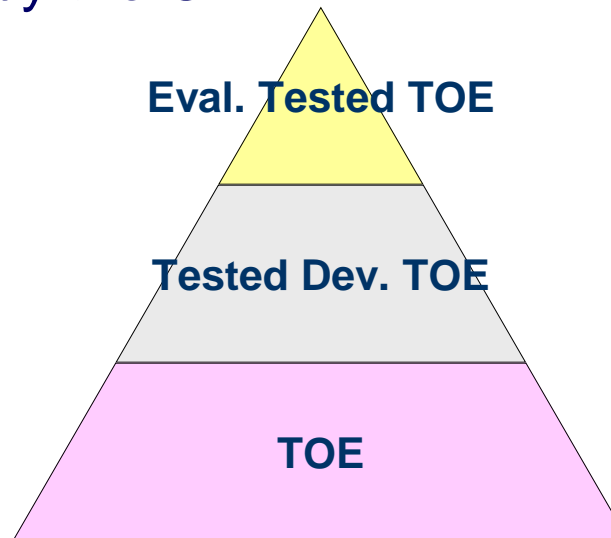


Vulnerabilities exploitation

- **TOE switched in internal state to an unsecure and unexpected state in which vulnerabilities could be exploited:**
 - By attack on boundaries,
 - Or unexpected command flow (not specified in specifications).



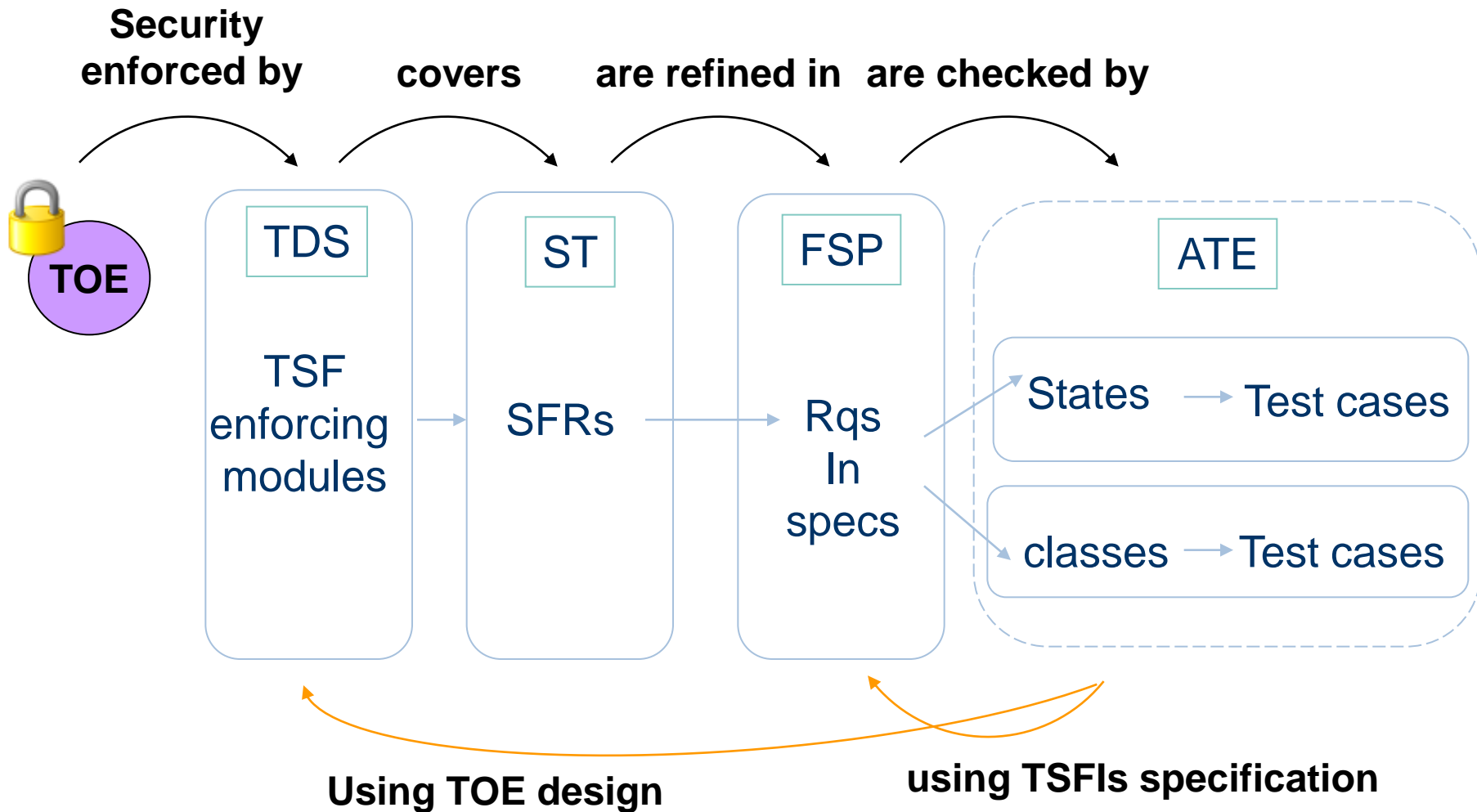
- As a first step, the developer provides a sampling of the possible tests.
- The evaluator proceeds to another sampling of this sampling as it is recommended by the CEM



The following will explain our sampling strategies



Test strategy and ATE methodology



- **The developer is going to organize the testing strategy**
 - How to select some representative security features
 - Testing strategy of error cases
 - How gaining confidence on command flow processing



Restricting the scope

SFRs usually map to full TOE

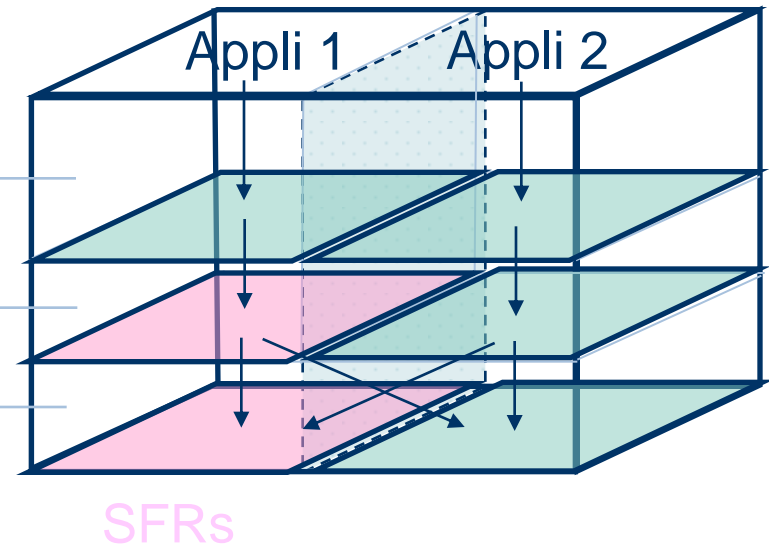


But in depth a subset of the full TOE can be considered

Application
non-sensitive layer

Application
secure layer

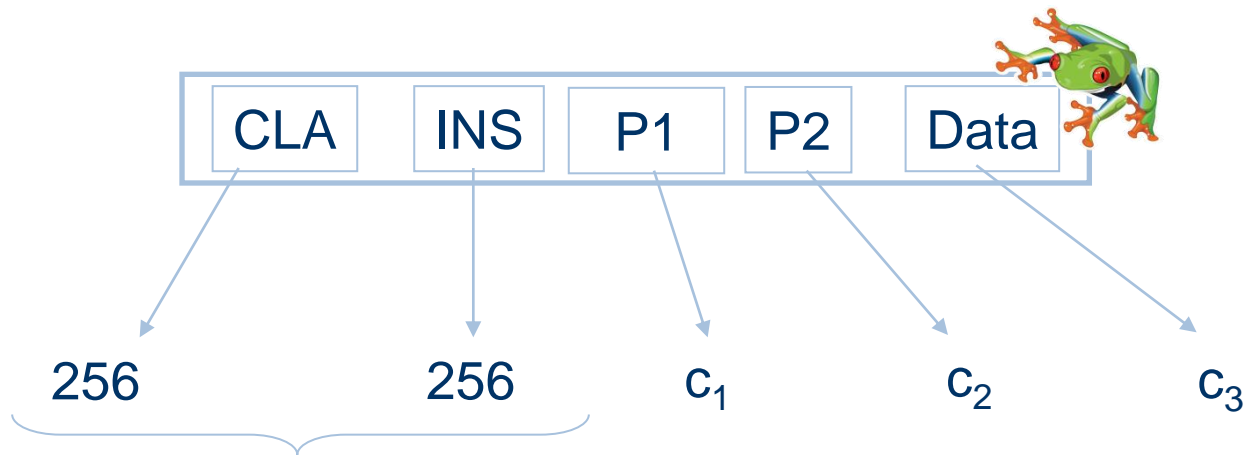
OS
secure layer



New methodology : Equivalence classes

Set of all elements which generate an equivalent behaviour

2 behaviours are equivalent if they are specified by the same requirement (same computation is performed, possibly on different values)



All behaviours are different:

- undefined → Fail 📱
- defined → ...P1,P2 and data to test

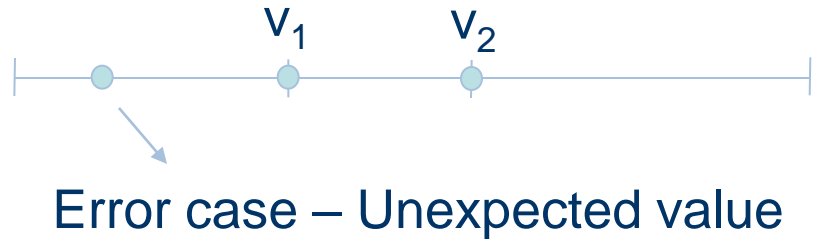


New methodology : Tests on ranges and discret values

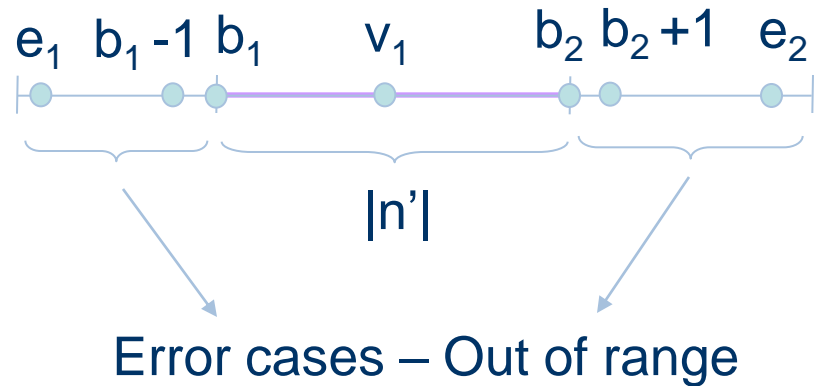
C_1 : 1 nominal behaviour / n values
In the full range



C_2 : 2 nominal behaviour / 2 values

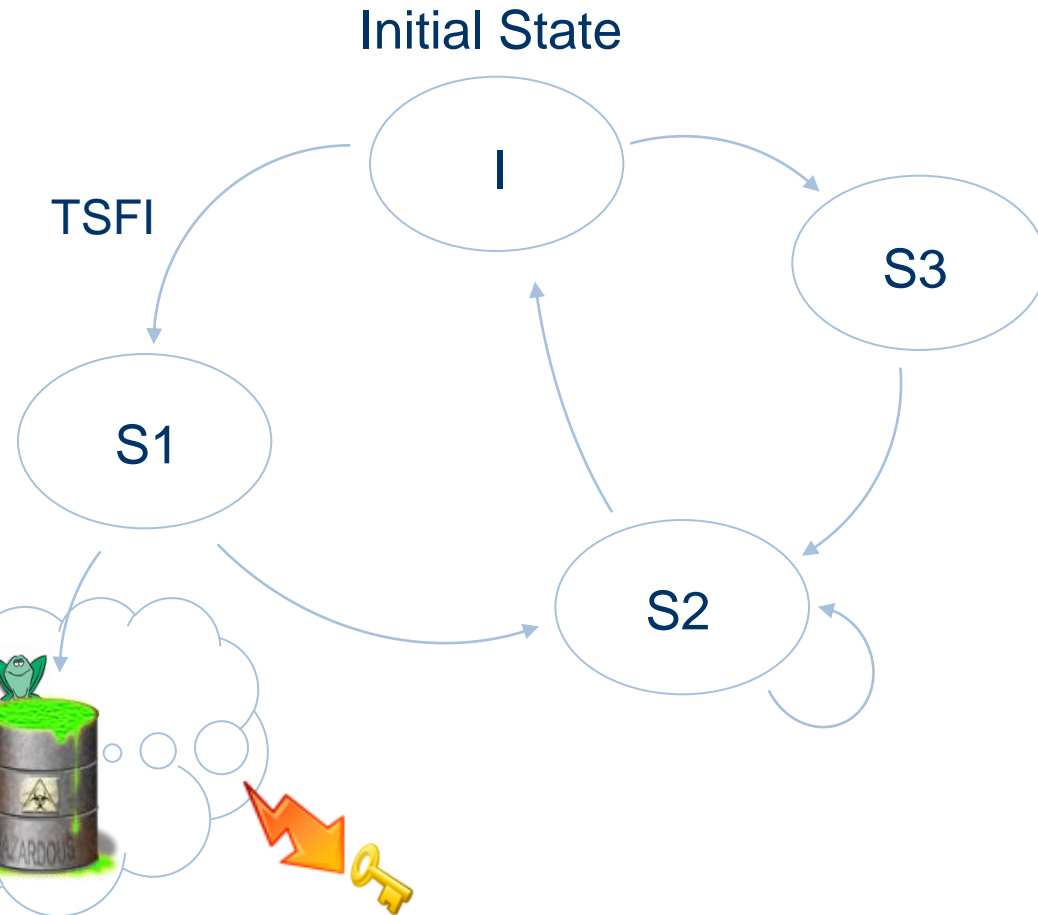


C_3 : 1 nominal behaviour / n' values
in a subset



New methodology : Smartcard state machine

- n states, n' transitions
- an infinity of path because of loops
- loop testing can be avoided
- 1 test by transition
- difficulty is to determine states
- Command flow testing is deduced from the state machine



Can be done by TDS
analysis of
dispatcher, global
variables and
memory access



- Developers call for an independent laboratory to perform functional tests or launch standardized test suites, the results can be reused as an entry of evaluation for nominal cases.
- A strategy defined by the developer which links requirements and tests to ensure a maximum coverage, focus on security.
- A methodology on the dispatcher dedicated to manage the external interfaces by analysis of TDS and IMP; then a well chosen sample of tests is defined.

The same process can be used by developer and evaluator

The evaluator resampling confirms the first results



- Using this approach of ATE offers the following good properties:
 - the evaluation work on tests can be easily adapted to the interface complexion and the scope of the TOE,
 - provides an assurance on tests that are not performed,
 - take into consideration the evaluation quality without adding too much time of evaluation.



Thank you!

