# ISE Task 3

# Specification of an evaluation process and framework definition

**ISE Seminar @ ETSI Security Week**

**16th JUNE 2017**

Projet porté par

Labellisation principale

Labellisations secondaires

Soutien de collectivités territoriales

- **Evaluating (IT) security is a “difficult” and expensive task**
  - Ever changing state of the art
    - New systems and technologies -> new attacks
    - Products lifespan very short
  - No universal scale/tests bed
  - Costly
    - Time consuming (complex systems)
    - Specific expertise (rare !?)
- **Very few internationally recognized evaluation schemes**
  - The Common Criteria (ISO 15 408) is the main reference
- **New to the automotive world**
  - The developer not used to it
  - The certification schemes not adapted yet to the automotive world

# State of the art : evaluation schemes

| Certification framework | Type of product | Certification Authority | ST | Assurance components / Evaluation scope | Evaluator | Tests on the TOE | Recognition | Assurance continuity | Duration and Cost |
|---|---|---|---|---|---|---|---|---|---|
| ITSEC | Any | National certification body | Defined by the level of evaluation | Security target evaluation, Life cycle, Development, Guidance documents, Functional Testing, Vulnerability testing | ISO 17025 accredited labs | Functional and vulnerability tests done by experts | Some EU members | Reevaluation | 6 months to several years |
| TCSEC | With the required functions | National certification body | To be written for the product | Development, Guidance documents, Functional Testing | - | | US | Reevaluation | 6 months to several years |
| CC | Any | National certification body | To be written for the product. Using CC standardized format | Security target evaluation, Life cycle, Development, Guidance documents, Functional Testing, Vulnerability testing | ISO 17025 accredited labs | Functional and vulnerability tests done by experts | CCRA signers up to EAL 2<br>SOG-IS members up to EAL 4 | Reevaluation | 6 months to several years |
| CSPN | Any | ANSSI | To be written for the product. Including all CSPN requirements | Guidance documents, Functional Testing, Vulnerability testing | Labs accredited by the ANSSI | Functional and vulnerability tests done by experts | France | Reevaluation | 25 days |
| EcoTaxe | ETS OBU | French DoT | No | Functional Testing, Vulnerability testing | ISO 17025 accredited labs | Conformance tests and security tests done by experts | France | Reevaluation | 1 year |
| FIPS | Cryptographic products | NIST and CSE | No | Development, Guidance documents, Functional Testing | Accredited as Cryptographic Module Testing laboratories by the National Voluntary Laboratory Accreditation Program. | Conformance tests | US and Canada | Reevaluation | 3 months to more than one year |

# Three main approches

- **Conformity checks**
  - E.g. FIPS
  - Need a reference conformity list
    - Has to be up to date
      - Difficult/industrially infeasible ?
  - Anything not conformant cannot be validated
    - No possible interpretation
    - No own interpretation
- **Vulnerability tests**
  - Adapted to the product regarding the state of the art
  - Low to medium assurance level
  - Needs to be confident in the tester
- **Assurance framework**
  - More complete and exhaustive approach
  - Provides the highest assurance level
    - From low to high
  - Costly and time consuming
  - Requires  accredited evaluators

- **Security Target (ST): What to evaluate?**
  - Which version of the product
  - Which function of the product
  - In which environnent, etc.
- **Assurance component: Which evaluation activities?**
  - Evaluate the development
  - Evaluate the product architecture
  - Test the external/internal interfaces
  - Analyze the code, the guides, etc.
- **Scheme: Who is responsible of/doing what?**
  - Evaluation authority
  - Sponsors of evaluation
  - Evaluation facilities / Evaluators
  - Developer
  - End user, etc.

## Project deliverables

- **L3.1 Definition of an evaluation process**
  - State of the art
  - Validation of CC evaluation as a basis
  - ISE evaluation process
    - Discussion and validation of each CC assurance components
      - Definition of the level regarding Day 1 and Autonomous needs
    - Competences and validation requirements
- **L3.2 Definition of an evaluation scheme**
  - Definition of required scheme processes and tools
    - Roles information access, Report delivery, Certificate emission and publicity, Communication interfaces
  - Definition of required roles and associated actors
    - PP developer, product developer, Integrator, site auditor, vulnerability tester
- **L3.3 and L3.4 Specifications for OBU's PP**
  - Security Problem definition
  - Security requirements
  - Assurance requirements

## Assurance Dimensions

- **Security Target (ST) ?**
  - Which version and test environnement
  - Which function of the system and why
  - Which function of the product and why
- **Assurance components ?**
  - Evaluate the development, the product architecture, test the external/internal interfaces, analyze the code, the guides, etc.
- **Scheme ?**
  - Roles
  - Activities per roles
    - Inputs/outputs
    - Required tools
  - Actors per roles

# The Reference in security assurance

## The Common Criteria

*for Information Technology Security Evaluation*

*(CC)*


Projet porté par

Campus Paris Saclay
Fondation de Cooperation Scientifique

Labellisation principale

SYSTEMATIC
Paris Region Systems & ICT Cluster

Labellisations secondaires

advancity
Ville & Mobilité Durables

ASTech
Paris Region

mov'eo

Soutien de collectivités territoriales

îledeFrance

Essonne
Le Conseil Général

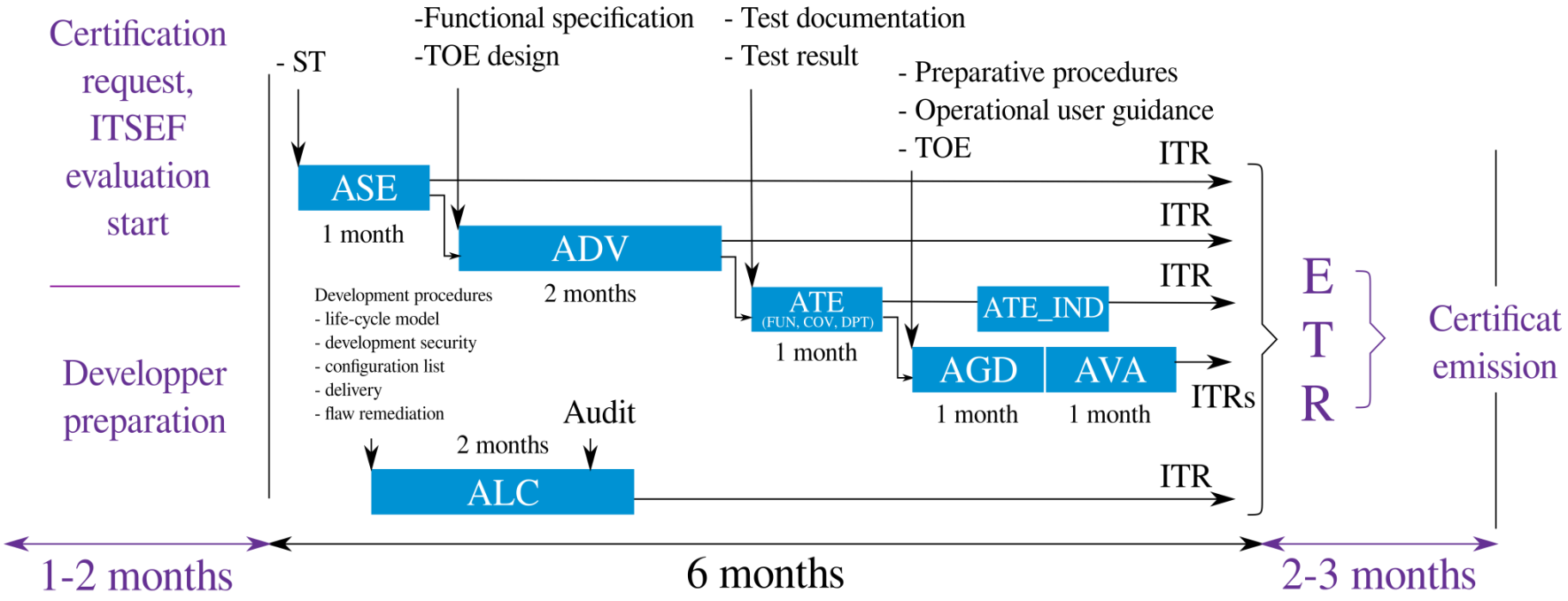
CAPS

- **From the ITSEF**
  - *Evaluation of assurance components on the Security Functional Requirements defined in the security Target (ST)*
    - For each iteration of assurance component, redaction of Intermediary Technical Report (ITR)
      - SUCCESS/FAIL or INCONCLUSIVE
    - At the end of the evaluation redaction of the Evaluation Technical Report (ETR)
      - Only when all ITR have SUCCESS status
- **From the Evaluation authority**
  - E.g. the prime minster in France
  - *Production of a certificate* stating that
    - An accredited body run a CC evaluation
    - Based on a specific ST
    - And the results of this evaluation was SUCCESS (i.e. no problem found during the evaluation)

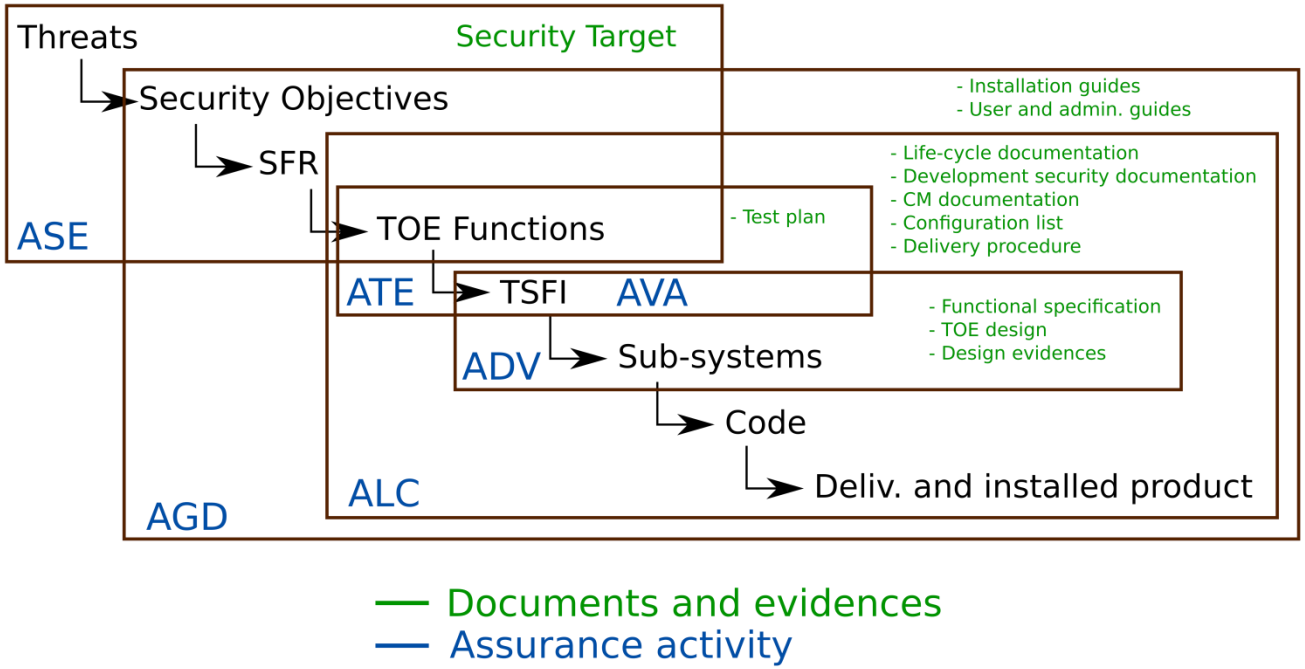
- **ASE - Security target Evaluation**
  - What must/has been evaluated (greatly enhanced by the use of PPs)
- **ALC - Life-Cycle support**
  - Development and the maintenance process of the TOE
    - Security measures to protect the integrity of the TOE design
    - There is a unique reference of the TOE and a precise list of the items used for the evaluation
    - Integrity of the TOE (and patches) during the delivery
    - (+) The developer can correct identified security flaws
- **ADV - DeVelopment**
  - Functional specifications
    - TSFI and accessible actions through these interfaces
  - Architecture description
    - TOE components (“sub-systems”)
    - Identify any vulnerability caused by design choices

- **AGD - Guidance Documents**
  - Transform the delivered object (cf. delivery procedures) into an operational TOE
  - Operate the TOE in use cases stated in the security target
- **ATE- TEsts**
  - The TSF interfaces (identified in ADV_FSP) have been tested and all TSFI and subsystems are covered by the tests
  - Check the results of the developer's tests
  - Perform if needed additional security-oriented tests
- **AVA - Vulnerability Assessment**
  - Identify potential vulnerabilities using all information gained during the evaluation
  - Test the exploitation of the potential vulnerability for an attacker with « basic » resources

# Getting from CC evaluation sequencing (EAL3+)...




Ideal schedule for developer used to CC evaluations and not too complex products .


Threats
Security Target
Security Objectives
- Installation guides
- User and admin. guides
SFR
- Life-cycle documentation
- Development security documentation
- CM documentation
- Configuration list
- Delivery procedure
ASE
TOE Functions
- Test plan
ATE
TSFI
AVA
- Functional specification
- TOE design
- Design evidences
ADV
Sub-systems
Code
Deliv. and installed product
ALC
AGD
Documents and evidences
Assurance activity

# ISE evaluation Framework

Projet porté par

Campus Paris Saclay

Fondation de Cooperation Scientifique

Labellisation principale

SYSTEMATIC

Paris Region Systems & ICT Cluster

Labellisations secondaires

advancity

Ville & Mobilité Durables

ASTech

Paris Region

mov'eo

Soutien de collectivités territoriales

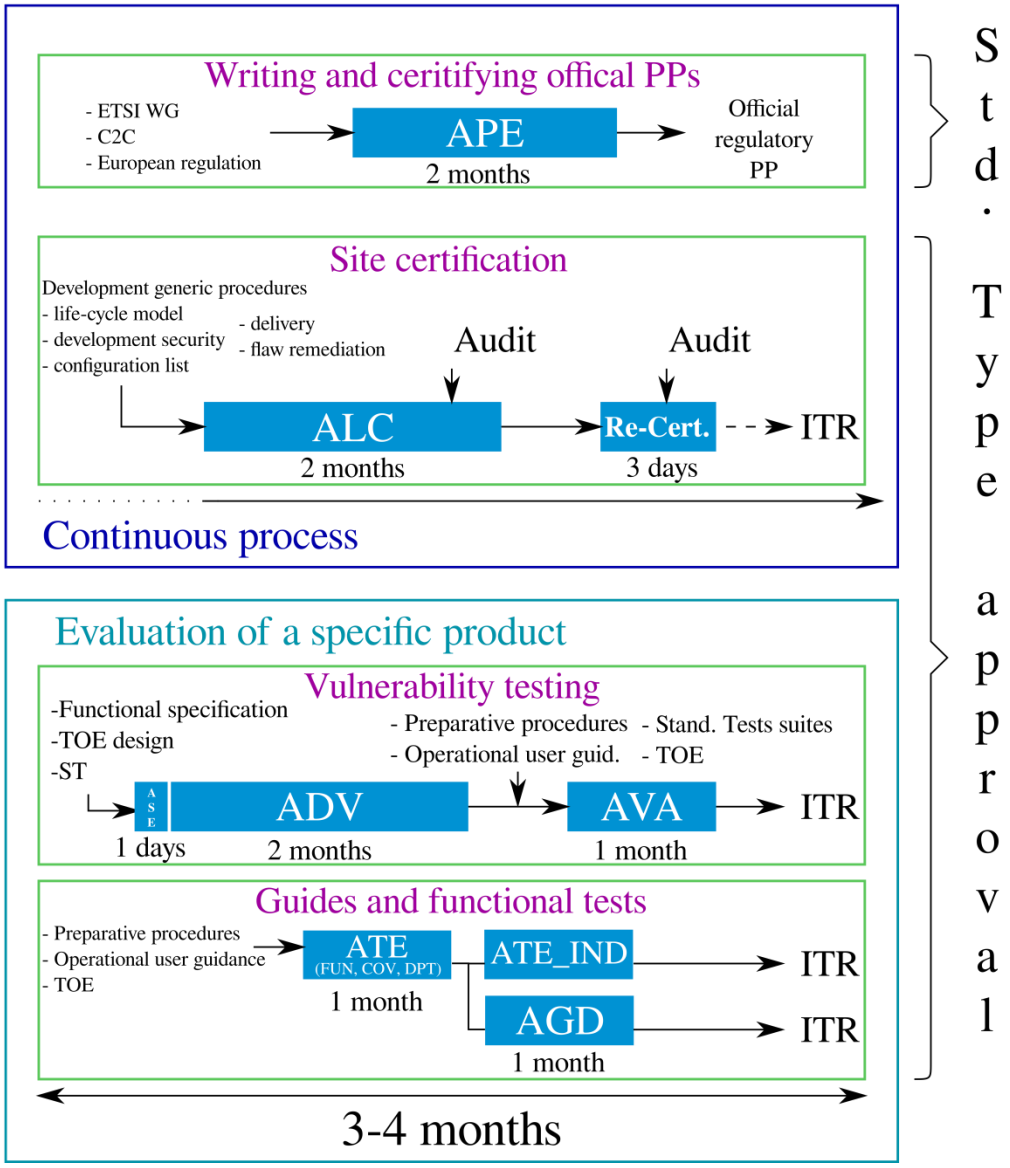
îledeFrance

Essonne

Le Conseil Général

CAPS

Parallelization of activities



- **Official/standardized ITS Protection Profiles**
  - Defined by official bodies
    - ETSI, DoTs, etc.
  - Based on community requirements and expertise
    - C2C, ETSI WG5, etc.
- **Evaluation tasks done in parallel**
- **Limited official and accredited bodies involvement**
  - No official certification body
    - Only type approval process
  - Licensed laboratory only for specific tasks
    - Vulnerability test
    - Developer security audits
    - Confidential industrial data (e.g. product architecture)

➢ **Lower costs (30%) and shorten evaluation time (40%)**

# Challenges and points of attention

Projet porté par

Campus Paris Saclay
Fondation de Cooperation Scientifique

Labellisation principale

SYSTEMATIC
Paris Region Systems & ICT Cluster

Labellisations secondaires

advancity
Ville & Mobilité Durables

ASTech
Paris Region

mov'eo

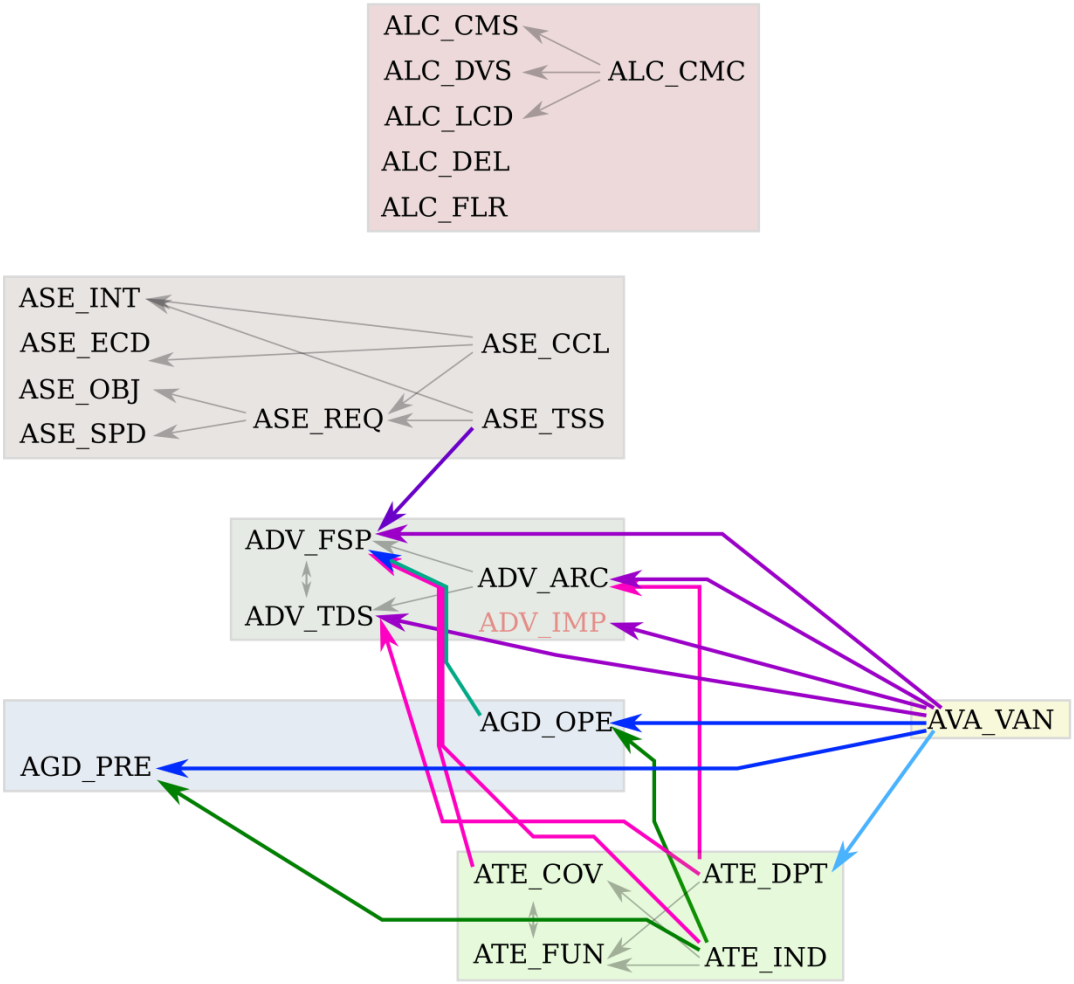
Soutien de collectivités territoriales

îledeFrance

Essonne
Le Conseil Général

CAPS

# Carefull with the assurance tasks depandencies



## A framework has been proposed but…

*Evaluation/validation of the economical model and feasibility feedback*

- **Define the current cost of an ITS development without security validation**
  - Estimated at 60-80% of actual real certification cost
- **Validate the feasibility of the solution**
  - Capacities of the developer(s) to provide proper inputs
- **Evaluate the current best practice reuse**
  - Identify for each evaluation input the nearest existing document and evaluate
    - The effort needed to adapt those documents to the proposed evaluation activities
    - Efforts to integrate them as best practices
- **Validate the CC tracing integration in the products lifecycle**

# Thank you for your attention

# Questions ?

sammy.haddad@oppida.fr

Projet porté par

Labellisation principale

Labellisations secondaires

Soutien de collectivités territoriales

# ISE security evaluation framework

| Assurance component name | Assurance component goal | To be used in our framework | | Evaluator constraints : Independence, Licensed expertise | Proposed actor |
|---|---|---|---|---|---|
| | | Day 1 | Autonomous | | |
| APE | PP writing | Yes | Yes | • Recognized community of experts | ETSI and ISO |
| | PP validation | Yes | Yes | • Regulation | European community |
| ASE | Validate the proper definition of the assurance assessment goal. | Yes | Yes | • No requirements | Product integrator (car manufacturer) |
| ALC_LCD.1 | Validate the proper control and quality of the life-cycle procedures | No | Yes | • Independent body<br>• Licensed laboratory | SOG-IS approved ISO 17020 or ISO 17025 ITSEF |
| ALC_DVS.1 | Validate the proper security (integrity and confidentiality) of the TOE during its developments | No | Yes | • Independent body<br>• Licensed laboratory | |
| ALC_CMC.1 | Validate the proper control of the TOE and its corresponding documentation versions. | No | Yes | • No requirements | Product integrator (car manufacturer) |
| ALC_DEL.1 | Validate the conformity and integrity of the product delivered to the car manufacturer | No | Yes | • No requirements | |
| ALC_FLR.1 | Validate the proper handling of flaw reports and remediation | No | Yes | • No requirements | |
| ADV_FSP | Enforce a good definition and control of the TOE functional specification and tracing of security functions for each of its interfaces. | FSP.2 | FSP.3 | • No requirements | Product integrator (car manufacturer) |
| ADV_TDS | Validate TOE design and decomposition into sub-systems and modules. | TDS.1 | TDS.3 | • Independent body | SOG-IS approved ISO 17025 ITSEF |
| ADV_ARC.1 | Validate the existence and relevance of security architecture choices. | No | Yes | • Independent body | |
| AGD_PRE.1 | Verify that the installation guides are correct and allow to install the TOE as defined in the ST | Yes | Yes | • No requirements | Product integrator (car manufacturer) |
| AGD_OPE.1 | To be able to operate the TOE securely and as defined in the ST | Yes | Yes | • No requirements | |
| ATE_FUN.1 | Verify that the developer tested the TOE. | Yes | Yes | • No requirements | Product integrator (car manufacturer) |
| ATE_COV.2 ATE_DPT.1 | Prove that all TSFI and subsystems are covered by tests | Yes | Yes | • No requirements | |
| ATE_IND.1 | Independently test the TOE to validate the developer test plan and gain knowledge and confidence in the product for the tester | Yes | Yes | • No requirements | |
| AVA_VAN | Identify and test the exploitation of potential vulnerabilities using all information gained during the evaluation | VAN.1 | VAN.3 | • Independent body<br>• Licensed laboratory | SOG-IS approved ISO 17025 ITSEF |