Risk Analysis and Security Assurance in Connected Vehicles: The SAFERtec and 2CeVau approach

Panagiotis Pantazopoulos, PhD
Senior Researcher,
Institute of Communication and Computer Systems (ICCS), Greece
E-mail: ppantaz@iccs.gr

9/20/2020

My Background in brief

- **2015 – now** Senior Researcher @Institute of Communication & Computer Systems, Greece
  - Intelligent Transport Systems
    - Cyber-security
    - ML applications
    - 5G test-bed and MANO optimization techniques

- **2008 – 2015** Researcher @National & Kapodistrian University of Athens
  - Service placement over ISP topologies
  - Delay tolerant networks
  - Network Science

- **Studies**: Bachelor in Physics, MSc Control & Computing, PhD Computer Networks

Presentation Overview

- Risk analysis
  - Basics and goals
  - Processes involved and methodologies
  - Applications on connected vehicles
- Security assurance
  - Why is it important?
  - Involved critical parameters
  - Similarities to SW testing
- The approaches so-far
  - Pros & Cons
- Spotlight on the Common Criteria standard
  - Highlights of the standard
  - The Protection Profile document & evaluation tasks

Concluding remarks

pointers to:

SAFER TEC

https://www.safertec-project.eu/

2CeVau

https://2cevau.eu/

THE RELEVANT PROJECTS IN A NUTSHELL

SAFER TEC

Project facts
Start date: January 2017
Duration: 39 months
Budget: 3.81 MEuros

Industry: AIRBUS DEFENCE & SPACE, CRF, swarco, TOMTOM
SMEs: Autotalks, OPPIDA, commsignia
Research Institutes: ΕΠΙΣΕΥ ICCS, UNIVERSITY OF PIRAEUS

Security Assurance Framework with V2I focus

- **Risk analysis** on challenging V2I use-cases
- Design of an agile **ITS assurance framework**
- Realization of the **use-cases on test-benches** with 3rd party software & hardware
- **Evaluation** of the framework's effectiveness
- Supporting the framework with an online toolkit
- Contribution to relevant standards

2CeVau

24-month CEF project
(01/08/2019 – 31/07/2021)

UNIVERSITY OF PIRAEUS RESEARCH CENTER
Πανεπιστήμιο Πειραιώς
University of Piraeus

ΕΠΙΣΕΥ ICCS

Cybersecure cross-border Corridor

HELLENIC REPUBLIC
Ministry of Digital Policy, Telecommunications and Media

- **Define the 5G corridor assets** to be protected by considering the connected vehicles together with the associated infrastructure/services.
- **Identify threats and potential vulnerabilities** that can compromise assets for the 5G corridor crossing.
- **Perform attack modelling** and **define countermeasures** able to protect system assets.
- **Develop a reporting-auditing assessment toolkit** that can be integrated in CSIRTs.

RISK ANALYSIS BASICS

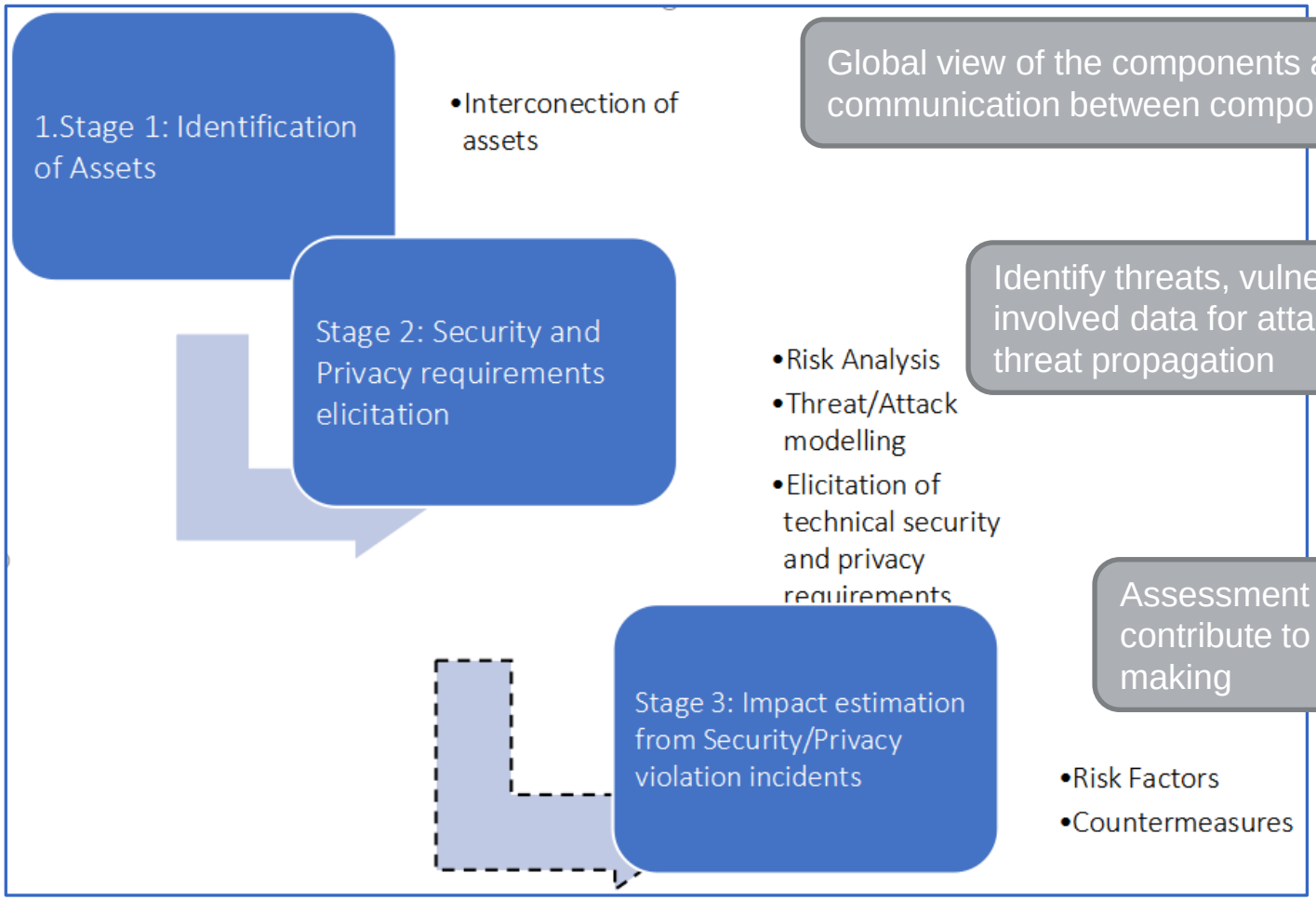
- **Asset** : any tangible or intangible thing or characteristic that has value to an organization.
- A **Threat** expressed as an **attack** or incident, represents circumstances that have the potential to cause loss or jeopardize the systems' security features
- A **Vulnerability** is defined as an (asset's) existing weakness in terms of security and privacy in a resource, actor and/or a goal

$$Risk = f(A, T, V)$$

Implications

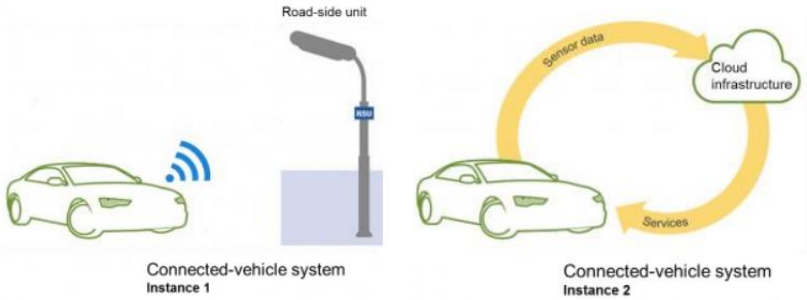
- ✓ ensure that necessary security and privacy objectives are integrated into the system design and implementation
- ✓ assess the impact and inform the decision-making on effective countermeasures/investments

RISK ANALYSIS BASICS: A STEPWISE APPROACH



How to Identify security & Privacy Requirements of Connected vehicles

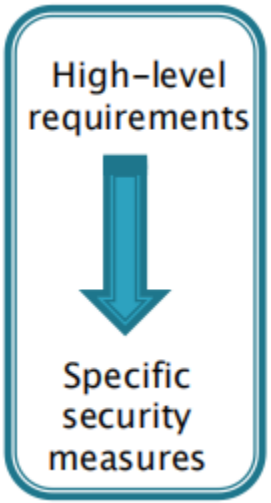
V2I use-cases



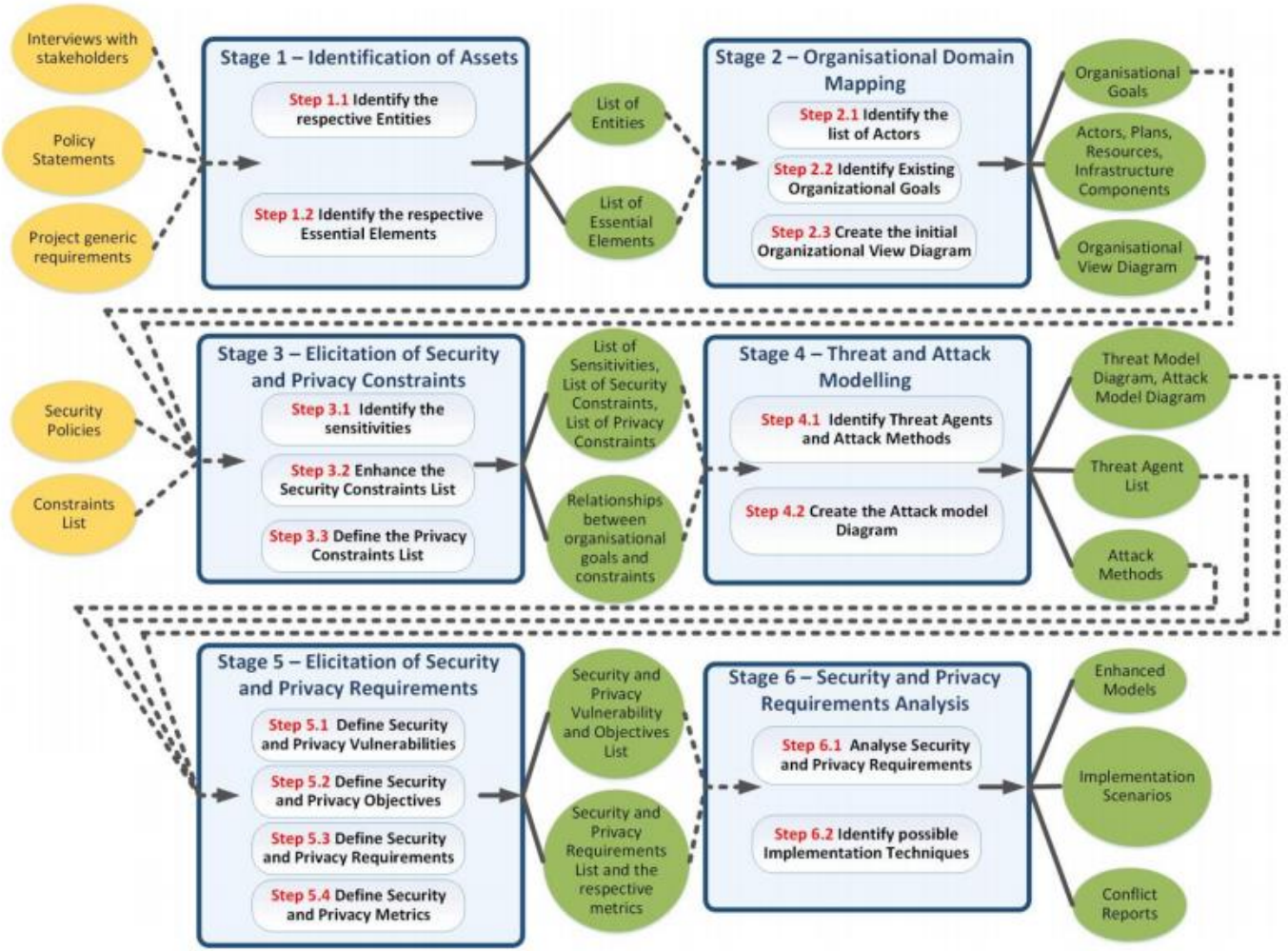
approach

- combination of three well-known approaches
- Bridge the gap between the design and implementation phases
- It combines risk analysis and attack modelling techniques

EBIOS	• Initial modeling (*i.e.*, identification of entities) and threat analysis
Secure Tropos	• Reasoning on security requirements
PriS	• Reasoning on privacy requirements

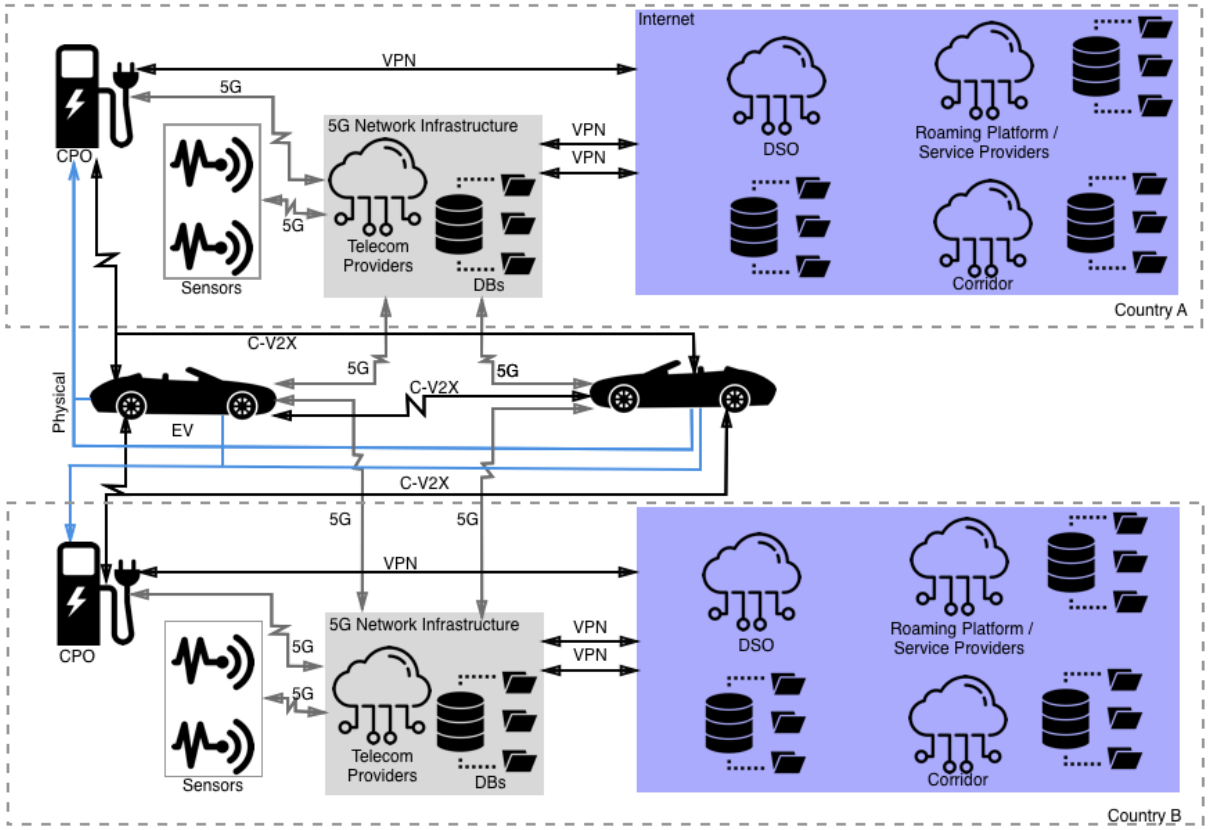


How to Identify security & Privacy Requirements of Connected vehicles



Each step consists of several steps

Risk Analysis For Cross-border and EV use-cases



What security requirements?

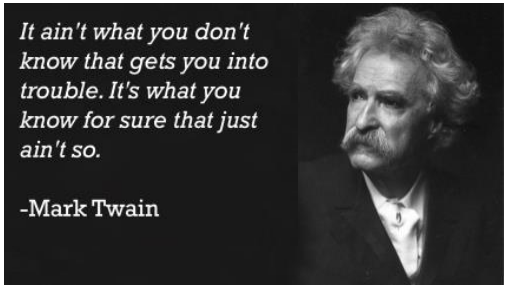
- Confidentiality
- Integrity
- Availability

In the (cross-border) automotive setting

- **Anonymity**: an attacker cannot sufficiently identify the subject within a set of subjects.
- **Unlinkability** of multiple items of interest (IOI): the attacker cannot sufficiently distinguish whether these IOIs are related or not.

2CeVau

SECURITY ASSURANCE: PROBLEM STATEMENT



(Cyber-)Security Assurance evaluation

- A “post-design/implementation” question
- establish trust that a system satisfies its intended cyber-security behavior
  - or
- the degree of confidence that the security requirements of an IT system are satisfied
- parallel lines with SW testing

a) What is to be evaluated?

b) Which evaluation activities to follow?

c) Which entity performs the evaluation activities?

SPECTRUM OF THE SOLUTIONS EFFICIENCY

do nothing Evaluation tasks **formal proof**

Proofs that system behaviour meets a desirable property
(e.g., show that no attack strategy in a class of strategies will cause a system to misbehave)

- formal proofs are increasingly-difficult if not infeasible, as complexity increases
- the question is what happens (practically) in-between the extreme values

→ a trade-off between efficiency and cost

Approaches to Security Assurance Evaluation

- **Vulnerability tests**
  - a quick perimeter definition
  - experts runs tests of their choice during a predefined time-period
  - depends on the expertise of the tester
  - comparison between tests

low to medium assurance level (in the product's security)

- **Conformity checks**
  - validates a system's compliance to a specific reference
  - fastest and cheapest evaluation scheme
  - a reference conformity list has to be kept up to date (occasionally cumbersome)
  - anything not conformant to a subset of this list cannot be validated

medium levels of assurance

APPROACHES TO SECURITY ASSURANCE EVALUATION

Get someone else to do the job and leave me alone!

- **Assurance framework**(s)
  - most complete and exhaustive one
  - requires a precise description of the evaluation objectives and requirements to prescribe dedicated and extensive evaluation activities
  - comes at the expense of considerable **cost** and time-to-complete
  - requires rare and expensive accredited evaluators

- **Common Criteria**
- ISO/SAE 21434
- FIPS 140-2
- Carsem *
- SAFERtec

(up to) **the highest level of assurance**

* S. Haddad, A. Boulanger, P. Cincilla, and B. Lonc, CARSEM: A Cooperative Autonomous Road-vehicles Security Evaluation Methodology. In 25th ITS World Congress, September 2018, Denmark.

Spotlight on Common Criteria (ISO/IEC 1540)

Risk analysis

- Target of Evaluation (ToE): the system to be evaluated
- **Protection Profile** (PP): Generic yet systematic definition of evaluation criteria for a generic type of product
- **Security Target** (ST): the document specifying TOE and the evaluation tasks
- The Security Functional Requirements (**SFR**): the specification of the security functions that the TOE must implement
- The TOE Security Functionality (TSF): the part of the TOE where the SFR are implemented
- The TSF Interfaces (TSFI): the interfaces used by the users to interact with the TSF
- **Assurance Levels**: EAL 1 to EAL7, each of them increasing the level of requirements and evaluation tasks to be undertaken on the TOE

The first version of the CC dates back to 1994

Inspired by previous assurance evaluation initiatives: TCSEC (US DoD), ITSEC (EU standard), the Canadian CTCPEC4

Last version standardized in 2009, 5 revisions ever since

PROTECTION PROFILES (IN COMMON CRITERIA)

Rationale

each security objective for the TOE (environment) covers at least one threat (or assumption)

- Adopts a certain structure and terminology to formally define the involved security functional requirements (SFRs) and security assurance requirements (SARs)
- Protection Profile (PP) describes requirements that are implementation-independent while the Security Target (ST) refers to one specific ToE implementation

PROTECTION PROFILES (IN COMMON CRITERIA)

FCS_CKM.4.1	**The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].**
FCS_COP.1.1	**The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].**

(components and) functional elements

FCS_COP.1.1	The **Hypervisor/OS** shall perform keyed-hash message authentication services in accordance with a specified cryptographic algorithm [**selection**: *SHA-1, SHA-256, SHA-384, SHA-512*] with key sizes [**assignment**: *key size (in bits) used in HMAC*] **and message digest sizes [selection: *160 bits, 256 bits, 384 bits, 512 bits*]** that meet the following: FIPS Pub 198-1 *The Keyed-Hash Message Authentication Code* and FIPS Pub 180-4 *Secure Hash Standard*.

Protection Profile

Security Target

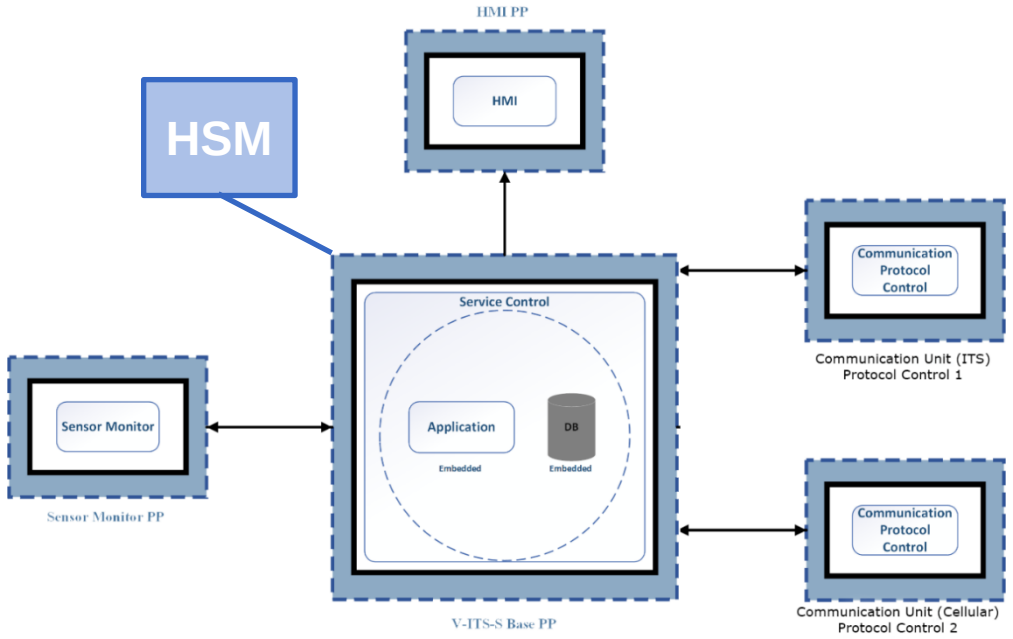
THE SAFERTEC MODULAR PROTECTION PROFILE

https://www.safertec-project.eu/publications/modular-pp/

- A generic architecture for a variety of implementations.
- A modular approach is followed in order to become more detailed and specific.

Modular-Protection Profiles consists of:

- Base Protection Profile
- Protection Profile module
- Protection Profile configuration



Modularity means

✓ *extensibility*
✓ *upgradability*
✓ *ability to integrate*

COMMON CRITERIA EVALUATION TASKS & PROCESS

- Security target evaluation [ASE class]
- Life-cycle [ALC class]
- Functional specification and architecture [ADV class]
- Functional tests [ATE class]
- Vulnerability analysis [AVA class]
- Guidance documents [AGD class]
- Composition [ACO class]

Risk analysis

THE SAFERTEC PROJECT CONTRIBUTIONS

- Introduction & evaluation of SAF (based on Common Criteria)
  - AOP class for composite evaluation
  - Dedicated knowledge base – Connected Vehicle **P**rotection **P**rofiles
  - Supported by an *innovative* risk analysis **generic methodology**
  - Dedicated online toolkit (for SAF/CC evaluations)

- Contribution to standards (as already *requested* in the DS-01-2016 call)
  - ETSI TVRA [*privacy issues*] **flagship standard**
  - EN 302 890-2/ Facility Position & Time [*proposal to extend the security requirements*]

- Design, implementation, integration and testing of two V2I testbeds
  - Advances State-of-the-Art by **realizing all V2I parts** (i.e., vehicle, RSU, cloud)
  - Served as the basis for the SAF experimental evaluation

- SAFERtec modular Protection Profile **online available**
  - Compatibility with standards (TVRA) and on-going industrial initiatives (Car2Car)

- AF Toolkit **cross-platform with code online available**

https://isense-gitlab.iccs.gr/safertec/aft

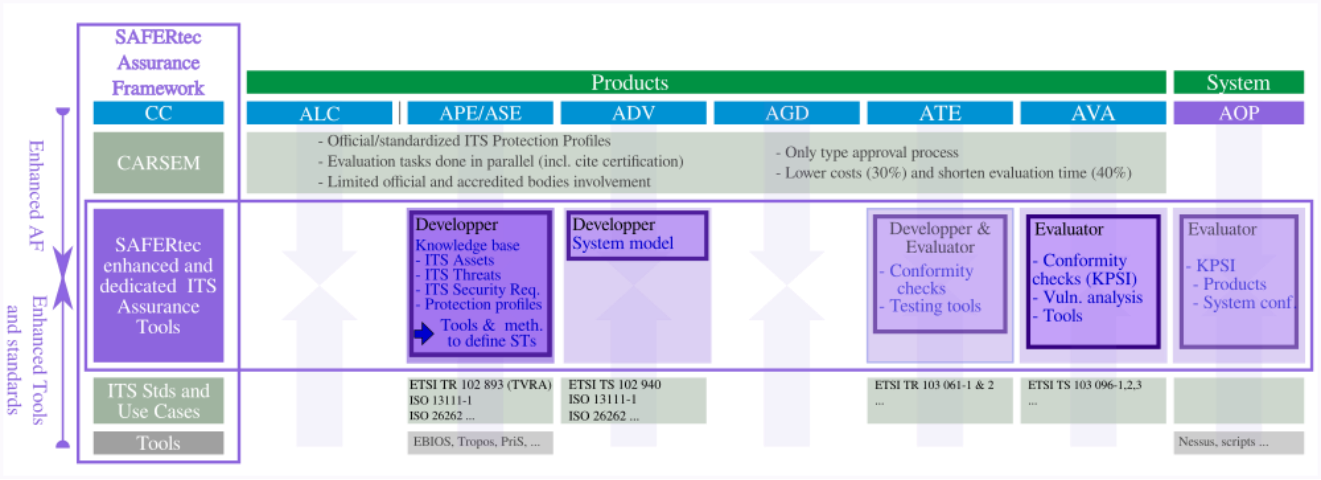
SOME 'TAKE-HOME' REMARKS

- Establishing vehicular connectivity comes with further cybersecurity, privacy and safety concerns
  - Uncertainty about achieving the security objectives is increased
- To gain confidence that automotive (cyber-)security controls will reduce the anticipated risks and involved high costs, we need:
  - (combination of) methodologies to elicitate security requirements
  - Efficient (dedicated) standards
    - Modularity in Protection Profiles
    - Enhancements to increase the cost-efficiency
- Risk analysis concrete results and security assurance research increase **trust** in connected vehicles/ITS

Contact Us!

Panagiotis Pantazopoulos,
Institute of Communication and Computer Systems,
Athens, Greece
✉ ppantaz@iccs.gr

SAFERtec Assurance Framework



- Dedicated ITS **Protection Profiles**
  - Based on community requirements and expertise
    - SAFERtec, C2C, ETSI WG5, etc.
  - To be standardized
- **Parallel** execution of tasks
  - Components vs system
  - Assurance by assurance task vs classical component certification
- **Limited** use of official and **accredited bodies** during evaluation…
  - No official certification body
    - Only type approval process
  - Licensed laboratory only for specific tasks
    - Vulnerability test, Developer security audits, Confidential data (e.g. product architecture)
- Providing **SAFERtec** dedicated tools for ITS security
  - Innovative combination of EBIOS, SecureTropos and PriS
  - WP6 tool box
- **Reduce the cost and shorten overall evaluation time**