SAFER TEC
SECURITY ASSURANCE FRAMEWORK FOR NETWORKED VEHICULAR TECHNOLOGY

Towards a Security Assurance Framework for Connected Vehicles

Panagiotis Pantazopoulos ICCS

Costas Lambrinoudakis UNIVERSITY OF PIRAEUS

Konstantinos Maliatsos UNIVERSITY OF PIRAEUS

András Váradi commsignia

Angelos Amditis ICCS

Sammy Haddad OPPIDA EXPERT EN SÉCURITÉ DES SYSTÈMES D'INFORMATION

Christos Kalloniatis UNIVERSITY OF PIRAEUS

Athanasios Kanatas UNIVERSITY OF PIRAEUS

Matthieu Gay AIRBUS DEFENCE & SPACE

IEEE SmartVehicles '18
5th WoWMoM Workshop on
Smart Vehicles: Connectivity Technologies and ITS Applications

Presentation break-down

- The considered problem and its importance

- Background

- Use-cases & elicitation of the security, privacy and safety requirements
  - Vehicle-to-Roadside station(V2R) and Vehicle-to-Cloud(V2R)
  - Modeling: innovative combination of three methodologies

- The proposed security assurance framework
  - Optimize Common Criteria (CC) to cope with the requirements of the connected vehicles paradigm

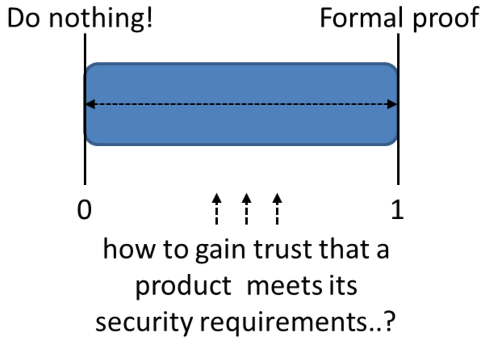
- The SAFERtec reference implementation (to act as a test-bed)

- (Experimental) evaluation processes of the framework

- Take-home remarks

The problem of Security Assurance

- Starting point: we can devise measures (e.g., encryption schemes) to mitigate threats but to what extent the system satisfies the intended (security) behaviour



how to gain trust that a product meets its security requirements..?

Under studied for 3 decades !

Potential cost of security incidents is large!

- Security assurance: the degree of confidence that the security requirements (Target of Evaluation) of an IT system are satisfied

- Assurance to provide confidence that a product enforces its security objectives without examining if those objectives appropriately address risks

A more general view: security evaluation schemes

- Different approaches to evaluate security placing emphasis on different aspects
- No ‘global’ solution - each one is criticised
- Three main solutions so-far:

Conformity checks

- Check compliance to a conformity list
- Maintenance issue and limitations from the list scope

Vulnerability tests

- Evaluation perimeter (any test of an expert’s choice)
- Depends much on the tester competences

Assurance frameworks

- More complete and exhaustive approach
- Costly and time–consuming
- High confidence

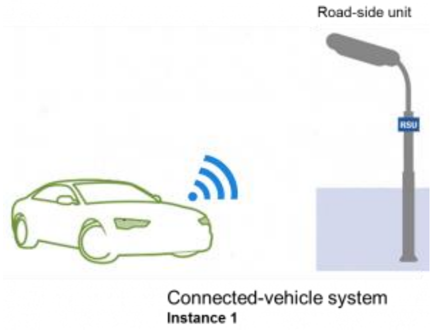
Common Criteria

What to evaluate?
Security Target

What evaluation activities?
-Architecture
-Interfaces
-Code

Who is in charge of what?
-Mgmt of activities
-Expertise & test environment

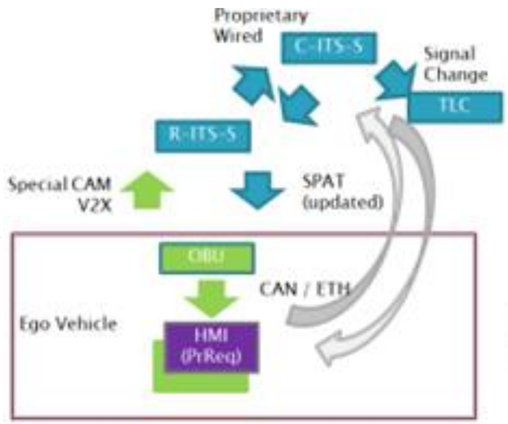
The automotive setting: use-cases (and involved entities)

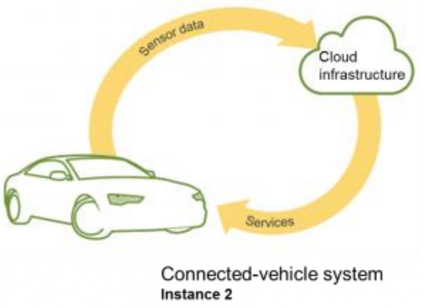


Connected-vehicle system
Instance 1

V2R

- Optimal driving speed advice (DSRC)
- Provision of real-time traffic-hazard information (DSRC)
- Priority request in intersection-crossing (DSRC + cellular)

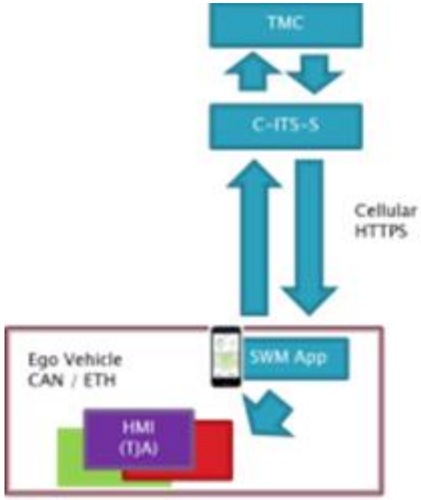




Connected-vehicle system
Instance 2

V2C

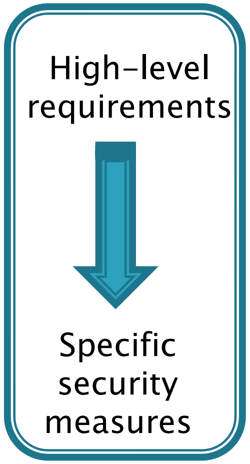
- Optimal driving speed advice (cellular)
- Provision of real-time information (cellular)
- Personalized provision of driving-advices (cellular)



How to identify the security, privacy and safety requirements (of the connected vehicles)?

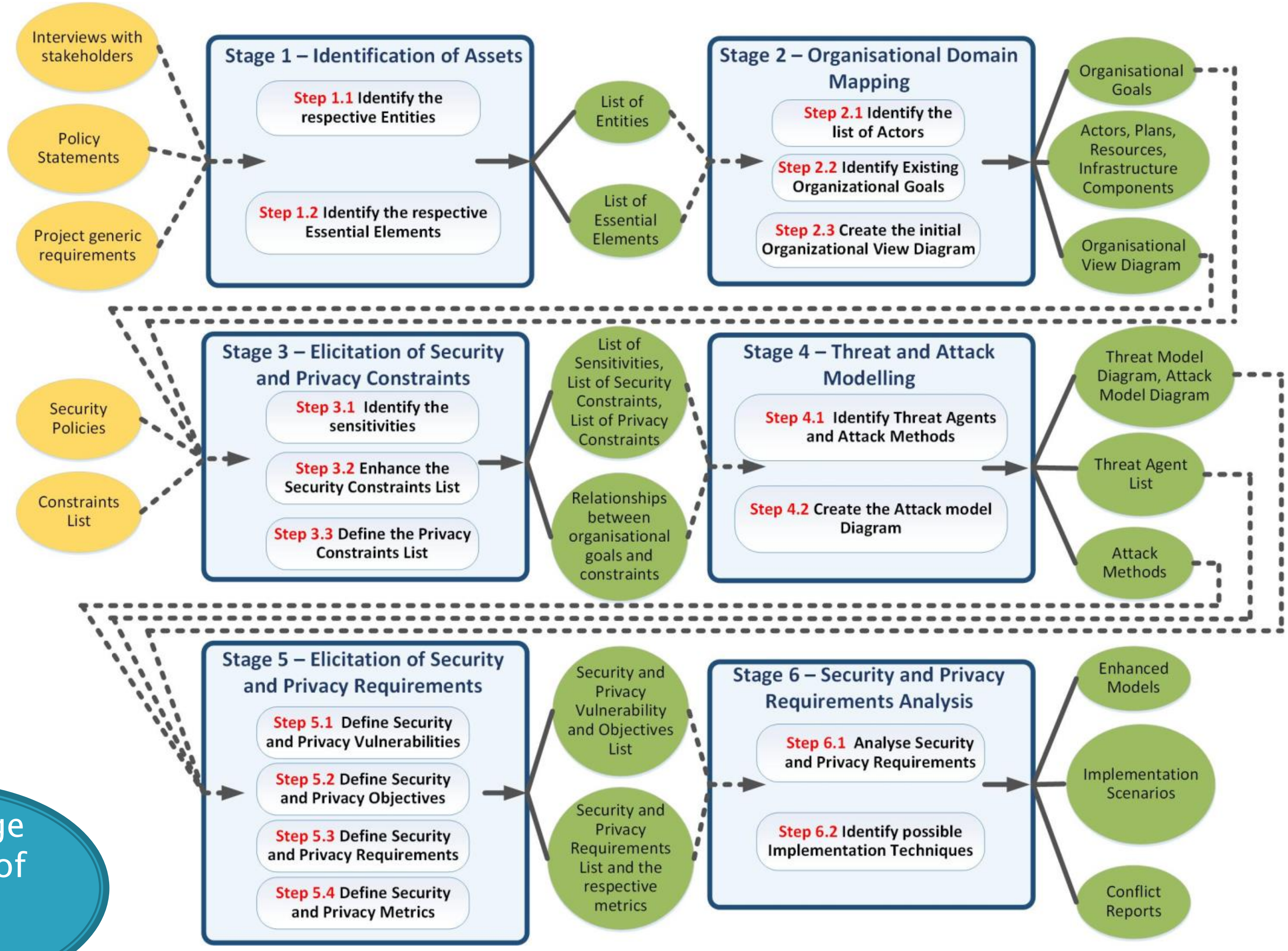
- Introduce a risk-based approach
- A Novel combination of three well-known approaches
  - Bridge the gap between the design and implementation phases
  - It combines risk analysis and attack modelling techniques

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


High–level requirements

Specific security measures

How to identify the security, privacy and safety requirements (of the connected vehicles)?



Interviews with stakeholders

Policy Statements

Project generic requirements

Stage 1 – Identification of Assets

- Step 1.1 Identify the respective Entities
- Step 1.2 Identify the respective Essential Elements

List of Entities

List of Essential Elements

Stage 2 – Organisational Domain Mapping

- Step 2.1 Identify the list of Actors
- Step 2.2 Identify Existing Organizational Goals
- Step 2.3 Create the initial Organizational View Diagram

Organisational Goals

Actors, Plans, Resources, Infrastructure Components

Organisational View Diagram

Security Policies

Constraints List

Stage 3 – Elicitation of Security and Privacy Constraints

- Step 3.1 Identify the sensitivities
- Step 3.2 Enhance the Security Constraints List
- Step 3.3 Define the Privacy Constraints List

List of Sensitivities, List of Security Constraints, List of Privacy Constraints

Relationships between organisational goals and constraints

Stage 4 – Threat and Attack Modelling

- Step 4.1 Identify Threat Agents and Attack Methods
- Step 4.2 Create the Attack model Diagram

Threat Model Diagram, Attack Model Diagram

Threat Agent List

Attack Methods

Stage 5 – Elicitation of Security and Privacy Requirements

- Step 5.1 Define Security and Privacy Vulnerabilities
- Step 5.2 Define Security and Privacy Objectives
- Step 5.3 Define Security and Privacy Requirements
- Step 5.4 Define Security and Privacy Metrics

Security and Privacy Vulnerability and Objectives List

Security and Privacy Requirements List and the respective metrics

Stage 6 – Security and Privacy Requirements Analysis

- Step 6.1 Analyse Security and Privacy Requirements
- Step 6.2 Identify possible Implementation Techniques

Enhanced Models

Implementation Scenarios

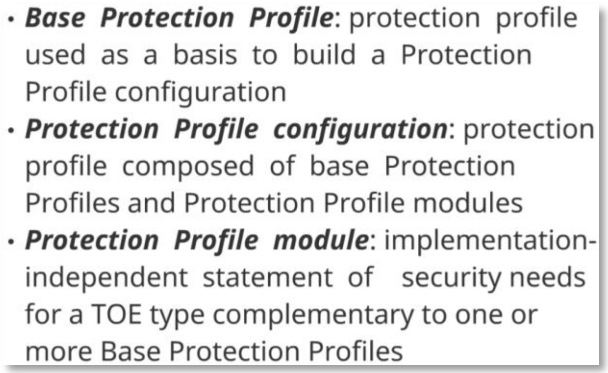
Conflict Reports

Each stage consists of several steps

The SAFERtec approach to automotive security assurance

- Rely on the most credible yet generic approach i.e., CC
  - Enhancements to meet the connected vehicles requirements
  - Efficient evaluation processes with less cost

- Main contributions
- Introduce a modular Protection Profile for the connected vehicle
  - Addressing TOEs with a variety of optional services and security features

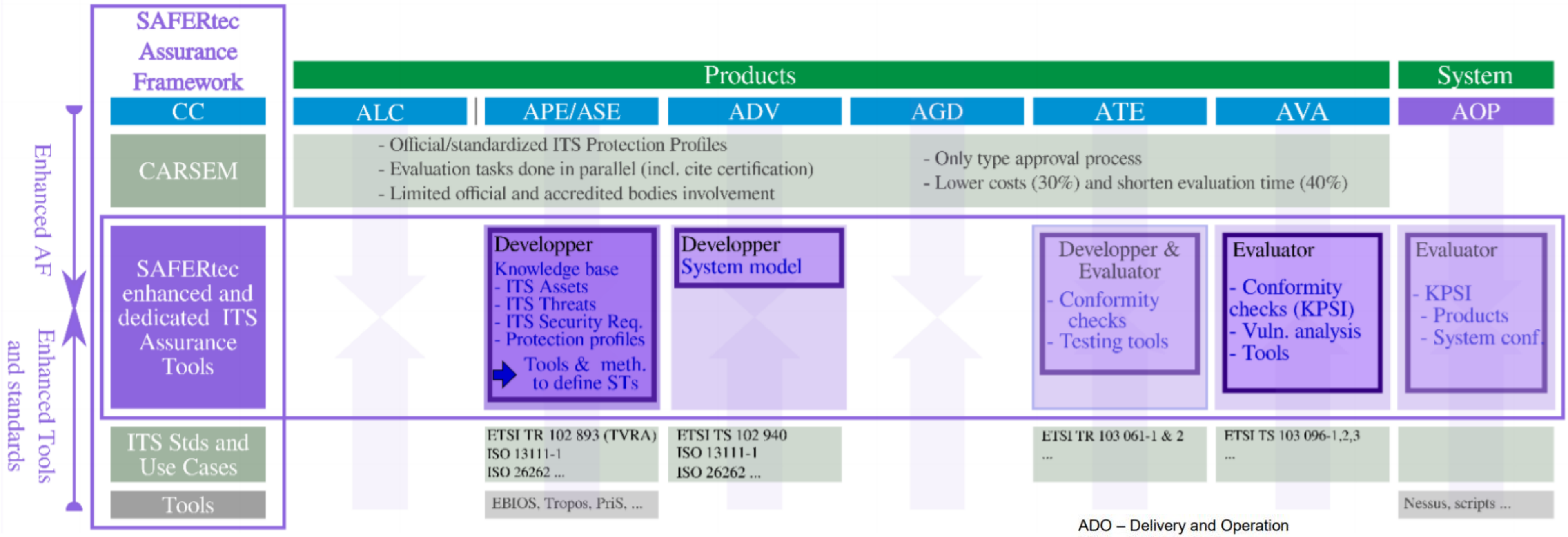


- ***Base Protection Profile***: protection profile used as a basis to build a Protection Profile configuration
- ***Protection Profile configuration***: protection profile composed of base Protection Profiles and Protection Profile modules
- ***Protection Profile module***: implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles

- Employ the idea of parallel execution of evaluation tasks and propose:
  - Dedicated tools and knowledge basis to ease the generation of reviews (by the developer)
  - Evaluation at system-level (AOP metrics)

The SAFERtec approach to automotive security assurance

- Example: ATE class (i.e., tests)
- Introduce: Metrics to quantify trustworthiness attributes of connected vehicles
  - To estimate the validity of a product & conformance to standards



SAFERtec Assurance Framework

Products

System

CC

ALC

APE/ASE

ADV

AGD

ATE

AVA

AOP

CARSEM

- Official/standardized ITS Protection Profiles
- Evaluation tasks done in parallel (incl. cite certification)
- Limited official and accredited bodies involvement

- Only type approval process
- Lower costs (30%) and shorten evaluation time (40%)

SAFERtec enhanced and dedicated ITS Assurance Tools

Developper
Knowledge base
- ITS Assets
- ITS Threats
- ITS Security Req.
- Protection profiles
Tools & meth. to define STs

Developper
System model

Developper & Evaluator
- Conformity checks
- Testing tools

Evaluator
- Conformity checks (KPSI)
- Vuln. analysis
- Tools

Evaluator
- KPSI
- Products
- System conf.

ITS Stds and Use Cases

ETSI TR 102 893 (TVRA)
ISO 13111-1
ISO 26262 ...

ETSI TS 102 940
ISO 13111-1
ISO 26262 ...

ETSI TR 103 061-1 & 2
...

ETSI TS 103 096-1,2,3
...

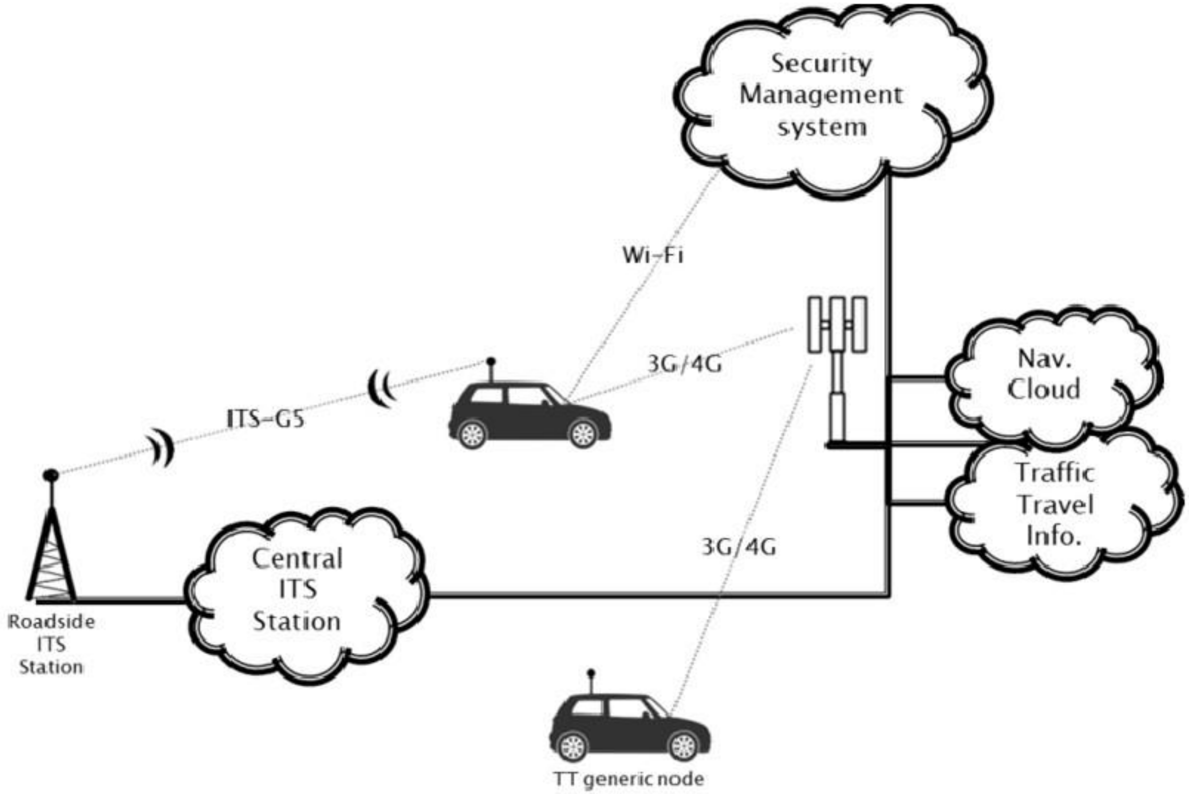
Tools

EBIOS, Tropos, PriS, ...

Nessus, scripts ...

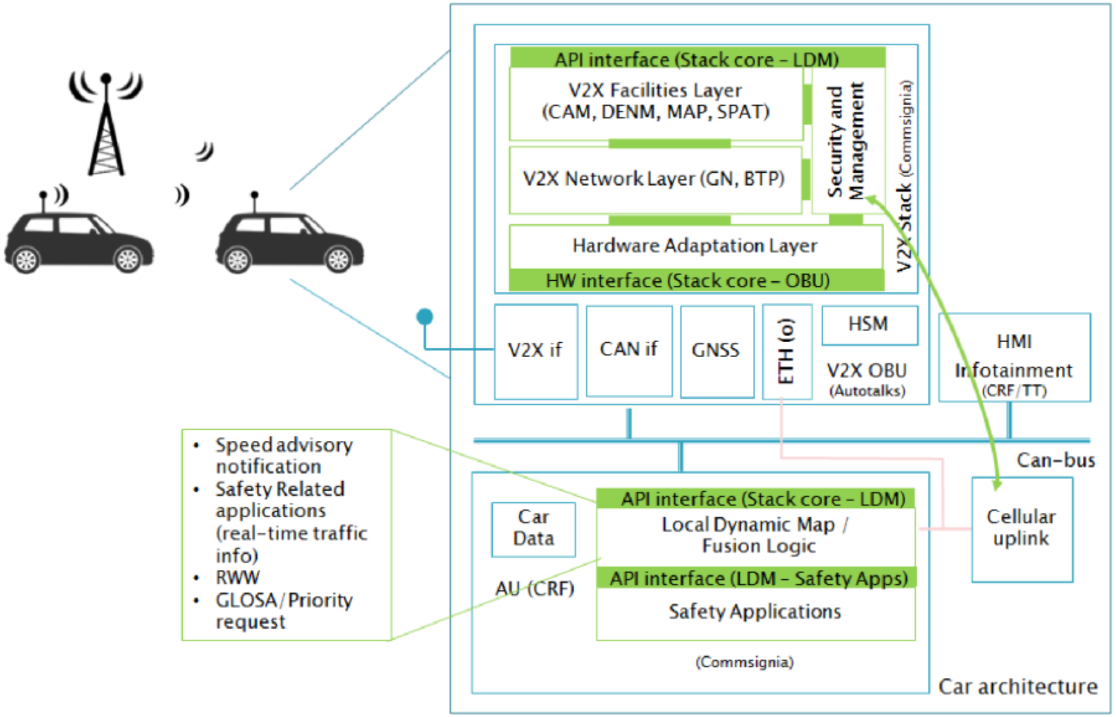
ADO – Delivery and Operation
ADV – Development
AGD – Guidance Documentation
ALC – Life Cycle
ATE – Tests
AVA – Vulnerabilities Assessment
AMA – Maintenance of Assurance

“Connected Vehicle System”: a reference implementation



- A prototype vehicle communicating with RSU and cloud-based services
- Realize the use-cases and act as a test-bed for the assurance framework evaluation

The in-vehicle architecture in more detail

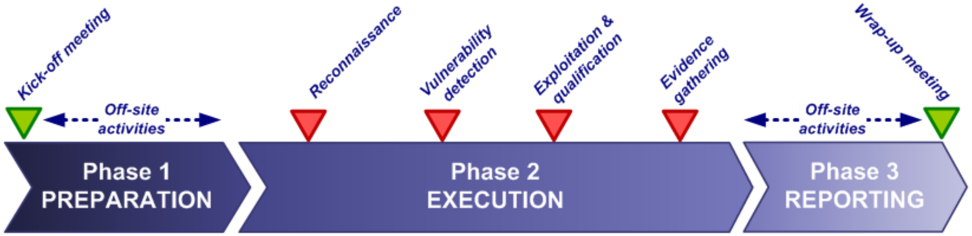

API interface (Stack core – LDM)
V2X Facilities Layer (CAM, DENM, MAP, SPAT)
V2X Network Layer (GN, BTP)
Security and Management
V2X Stack (Commsignia)
Hardware Adaptation Layer
HW interface (Stack core – OBU)
V2X if
CAN if
GNSS
ETH (o)
HSM
V2X OBU (Autotalks)
HMI Infotainment (CRF/TT)
Can-bus
Speed advisory notification
Safety Related applications (real-time traffic info)
RWW
GLOSA/Priority request
Car Data
AU (CRF)
API interface (Stack core – LDM)
Local Dynamic Map / Fusion Logic
API interface (LDM – Safety Apps)
Safety Applications
(Commsignia)
Cellular uplink
Car architecture

- On-board unit connected to the vehicle’s Controller Area Network
- ETSI ITS G5 integrated protocol stack processes and verifies incoming data from road-side station

Experimental evaluation of the proposed assurance framework

- Experiments (i.e., pen-testing) comes after a number of evaluation processes

- Penetration tests under a varying level of information availability
  - White box
  - Grey box
  - Black box



- Phase 2 is iterative
  - Detected vulnerabilities are quantified under CVSS

- Results to be used for updating the proposed assurance framework

Take-home remarks

- Establishing vehicular connectivity comes with further cyber-security, 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 have:
  - Introduced a combination of methodologies to elicitate security requirements
  - Proposed modular protection profiles
  - Enhanced the so-far most credible assurance framework to become more cost-efficient

- The proposed framework advances the (V2I) security assurance research aiming to increase trust in connected vehicles/ITS

Thank you!

Any Questions?

See details at
https://www.safertec-project.eu/

"This work is a part of the SAFERtec project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319"

Panagiotis Pantazopoulos

ppantaz@iccs.gr

Institute of Communication and Computer Systems (ICCS)
Athens, Greece