D5.4 Composite Evaluation of SAFERtec Assurance Framework

Security Assurance Framework for Networked Vehicular Technology

Abstract

SAFERtec proposes a flexible and efficient assurance framework for security and trustworthiness of Connected Vehicles and Vehicle-to-I (V2I) communications aiming at improving the cyber-physical security ecosystem of "connected vehicles" in Europe. The project will deliver innovative techniques, development methods and testing models for efficient assurance of security, safety and data privacy of ICT related to Connected Vehicles and V2I systems, with increased connectivity of automotive ICT systems, consumer electronics technologies and telematics, services and integration with 3rd party components and applications. The cornerstone of SAFERtec is to make assurance of security, safety and privacy aspects for Connected Vehicles, measurable, visible and controllable by stakeholders and thus enhancing confidence and trust in Connected Vehicles.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

DX.X & Title:	**D5.4 Composite Evaluation of SAFERtec Assurance Framework**
Work package:	WP5 Assurance Framework Evaluation
Task:	T5.3 Composite Evaluation
Due Date:	31-03-2020
Dissemination Level:	PU
Deliverable Type:	R

Authoring and review process information	
EDITOR	**DATE**
Guillemette MASSOT / CCS	28-02-2020
CONTRIBUTORS	**DATE**
Matthieu GAY / CCS	20-03-2020
Sammy HADDAD / OPP	02-03-2020
Kostas MALIATSOS / UPRC	25-03-2020
Panagiotis PANTAZOPOULOS / ICCS	24-04-2020
Sammy HADDAD / OPP	04-05-2020
REVIEWED BY	**DATE**
Leo MENIS / AUT	06-05-2020
Alessandro MARCHETTO / CRF	05-05-2020
LEGAL & ETHICAL ISSUES COMMITTEE REVIEW REQUIRED?	
NO	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Document/Revision history

Version	Date	Partner	Description
V0.1	28/02/2020	CCS	First draft
V0.2	02/03/2020	OPP	Deliverable structure update and refinement
V0.3	20/03/2020	CCS	Contributions on section 2
V0.4	25/03/2020	UPRC	Contributions on subsections 3.1 and 3.2
V0.5	28/03/2020	CCS	Refinements of subsection 2.1 and contributions on subsection 3.3
V0.6	15/04/2020	CCS	Refinements in all sections
V0.7	24/04/2020	ICCS	Corrections and refinements in all Sections, Inputs to Section 5
V0.8	04/05/2020	OPP	Contribution on Section 4
V0.9	04/05/2020	CCS	Take into account of corrections
V0.10	06/05/2020	CCS	Refinement of the deliverable taking into account reviewers' comments

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Table of Figures

List of Tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Acronyms and abbreviations

Abbreviation	Description
ACO	Assurance COmposition
AOP	OPerational Assurance
CAP	Composed Assurance Package
CC	Common Criteria
CEM	Common Methodology for information technology security Evaluation
CVS	Connected Vehicle System
CVSS	Common Vulnerability Scoring System
EAL	Evaluation Assurance Level
HSM	Hardware Security Module
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
ITS	Intelligent Transportation System
IVN	In-Vehicle Network
OBU	On-board Unit
OEM	Original Equipment Manufacturer
OS	Operating System
PP	Protection Profile
SAF	Security Assurance Framework
SFR	Security Functional Requirement
ST	Security Target
TOE	Target Of Evaluation
TRL	Technology Readiness Level
TSFI	TOE Security Function Interface
V-ITS-S	Vehicle - Intelligent Transportation System - Station

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

V2X	Vehicle-To-Everything

Table 1: List of Abbreviations

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Executive Summary

The present deliverable entitled “D5.4 Composite Evaluation of SAFERtec Assurance Framework” presents the outcome of task T5.3 named “Composite Evaluation” within the WP5 “Assurance Framework Evaluation”.

The evaluation of the security level of a system is a very complex task that comes out to be expensive and time consuming. In addition, this complexity grows with the complexity of the system to evaluate. In the case of a system composed of several sub-systems such as the Connected Vehicle System (CVS), the evaluation becomes difficult and relying only on already evaluated sub-systems is not enough to benefit from those evaluations and to draw conclusions for the composed system.

A connected vehicle is concerned by the mentioned points as car manufacturers integrate many devices and software systems together coming from different (Tier-1 or Tier-2) providers and typically try to guarantee the security level of the resulting CVS system. The state-of-the-art of assurance composition is restricted so far to the approach described in the Common Criteria class ACO (for Assurance Composition) at least in the best of the knowledge of the writers of this deliverable. Even though this approach is the only one available, it does not have been successfully applied yet (especially in the automotive domain). This is mainly due to the very strong constraints which turn-out to be incompatible with practical use cases.

After having presented the state-of-the-art of the assurance composition and relevant best practices, this document will detail the composite evaluation approach of SAFERtec that has been carried out throughout the project.

The definition of the SAF is based on general best practices (cf. section 2.2) to use them as follow. First, we used a top-down approach to derive the Security Functional Requirements of the identified critical components from our system-level risk analysis. This allowed us to directly take into account composition constraints by identifying security requirements for each component. Second, we applied a bottom-up assurance validation process, starting by assessing separately that each component met its security requirements. Then, we introduced some extra verifications issued from the top-down approach used for defining the security requirements; thus, we were able to check that related components were well-configured and that their interconnection in the integrated CVS did not cause further vulnerabilities.

Finally, to prove the relevance of the SAFERtec methodology for composition assurance, partners tested the composed (i.e., integrated) Connected Vehicle System developed in WP4 in order to identify possible weaknesses at system-level. The deliverable at hand presents preliminary evidence that SAF provides assurance at system-level. However, it is to be noted that our results even if promising, are preliminary and do not provide a full validation for the considered Targets Of Evaluation (TOEs); further observations and testing of our proposal are suggested to strengthen the validity of assurance arguments at system-level.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 732319

1 Introduction

This deliverable deals with the composite (or system-level) evaluation of the SAFERtec Assurance Framework (SAF). After having introduced the state-of-the-art of the security assurance composition, which is limited (in the best of our knowledge) to the Common Criteria ACO class and the best practices in this field, it will present how SAF provides efficient assurance composition.

First, the deliverable presents the risk analysis which allows to identify risks pertaining to the Connected Vehicle System (CVS). Using a top-down approach, this list of system-level risks is used to define the protections to be provided by the system to cover these risks, named system Security Objectives, which have subsequently shaped the Security Functional Requirements (SFRs) for the CVS. These SFRs are countermeasures that mitigate the system-level threats and allow implementing the Security Objectives. With the SFRs at hand and the identification of required security controls (to cover them), we obtain a projection of the identified system requirements over each CVS's critical components. In practice, this leads to the identification of the 'composition constraints' referring to the implementation of security measures and how they have to interact locally, in each module (see Figure 1, left part). For instance, security measures such as: security interoperability (use of the same cryptographic algorithms, use of signature mechanisms and verification where needed, common data flow filtering rules), conformity of environmental constraints (common user profile management and format, time references, network filtering compatible rules), functional interoperability (type and frequency of data exchanges, network protocols, compatible communication standards implementations). That data are taken into account for the security assurance validation that follows.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

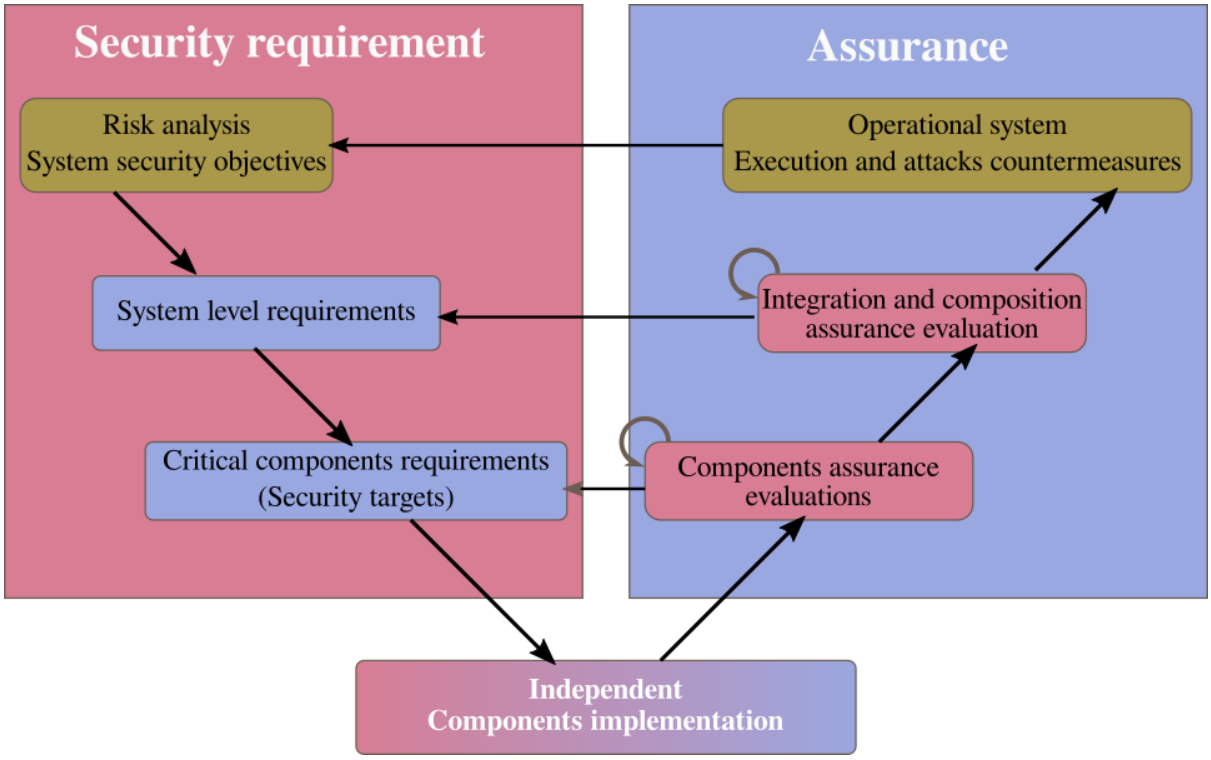

Figure 1: The SAFERtec V-shape approach to global evaluation

The bottom-up assurance validation process (see Figure 1, right part) starts by evaluating separately components before realizing extra verification of the components' (modules) configuration to check if those components are ready to be interconnected with others without creating security breaches. These two steps, the components assurance evaluations followed by extra tests to evaluate integration and composition of components, need to be iterative building upon the results of each evaluation cycle.

Finally, the deliverable gathers results from system-tests carried-out on the Connected Vehicle System developed in WP4 to identify if vulnerabilities due to composition (i.e., integration) of components can emerge and be found, in order to validate the relevance of SAF for assurance composition.

1.1 Purpose of the Document

The present deliverable entitled "D5.4 Composite Evaluation of SAFERtec Assurance Framework" presents the outcome of the task T5.3 named "Composite Evaluation".

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

1.2 Intended readership

In addition to the project reviewers, this deliverable is addressed to any interested reader (i.e. Public dissemination level).

1.3 Inputs from other projects

This deliverable does not use any inputs from other projects.

1.4 Relationship with other SAFERtec deliverables

This deliverable received inputs from SAFERtec work appearing in other deliverables. Specifically, the deliverables from the WP2 (D2.2, D2.3 and D2.4) for the risk analysis, the deliverables from the WP3 (D3.1, D3.2 and D3.3) for the definition of the SAF and its evaluation and the deliverable of the WP5 (D5.2 and D5.3) for composite evaluation.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

2 State-of-the-art of Composite Evaluation

The aim of this section is to describe the state-of-the-art of composition evaluation and especially to highlight the small number of existing approaches even if there is a real industrial need. The need of composition evaluation is especially high in the automotive sector where car makers should integrate separately secure components from several (third-party) providers while guarantying the security of the resulting integrated vehicle.

The well-known composition approach is the ACO class proposed by the Common Criteria [1] for Assurance Composition which is not fully recognised as there is (for the moment) no proof of its efficiency compared to the re-evaluation of the composed product. In the following section, we detail the ACO class.

2.1 Common Criteria – Class ACO – Composition

2.1.1 Presentation

The assurance level evaluation of any product relies mainly on the Common Criteria (CC). It is a set of norms that has been created in 1999 at the initiative of Canada, the United States of America and the European Union. Nowadays, it is widely recognised across the world by many countries either actively participating in the development of the CC or only recognising the standard and its usage.

CC are divided into 3 parts: the first one is an introduction which establishes the concepts and principles used, the second one deals with Security Functional Requirements and the last one is dedicated to the Security Assurance Requirements.

This third part defines two scales: one for measuring assurance for Targets Of Evaluation (TOEs) named Evaluation Assurance Levels (on 7 levels from EAL1 to EAL7) and another one named Composed Assurance Packages (on 3 levels from CAP-A to CAP-C) for measuring assurance for composed TOEs.

Common Criteria define many assurance classes and have been regularly updated through the years to add more classes or to improve existing ones. Each class covers a specific topic.

The figure au-dessous shows the organisation of the CC document. Each class has a unique name and an introduction, which is a description of the class and a presentation of its scope. Then the class is composed by one or several families with a specific scope and precise objectives for each one. Then, each family is composed of one or several assurance components, which are the tasks that the evaluator shall perform during a CC evaluation.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

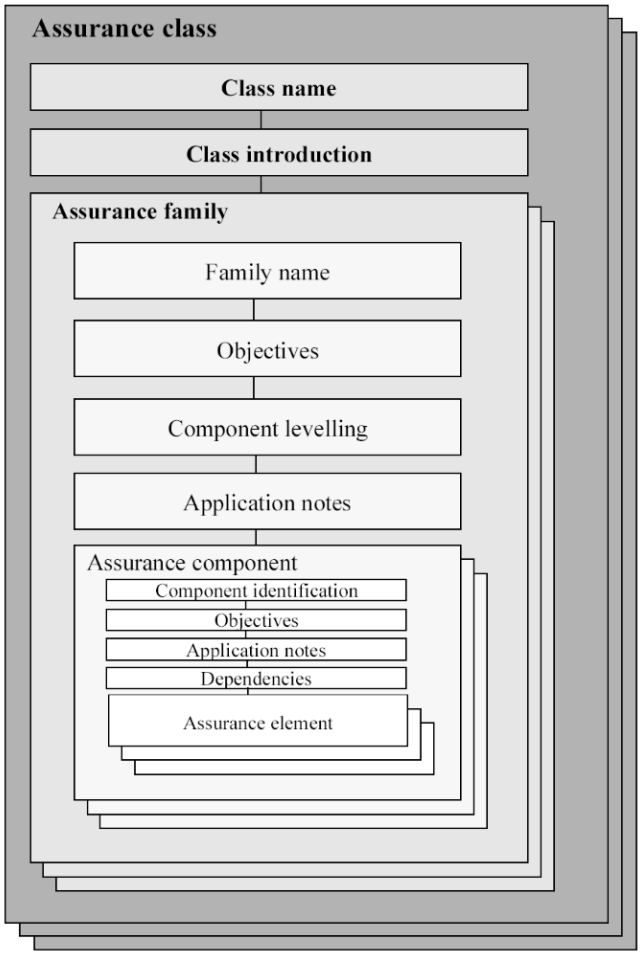

Figure 2: Assurance class/family/component/element hierarchy

Regarding the Assurance Composition, the class ACO has been introduced in 2005 in the version 3.0 of the CC. The last version of this class is available in the CC Part 3 (Security Assurance Components), published in April 2017 [1].

On the one hand, CC provide tools to measure assurance; on the other hand, the relevant Common Evaluation Methodology (CEM) [2] is a methodology that breaks down the actions that the evaluator must perform to carry out a CC evaluation. As the other classes, the ACO class follows the structure described in the Figure 2. It encompasses five families that are:

1. Composition Rationale (ACO_COR)
2. Development Evidence (ACO_DEV)
3. Reliance of dependent component (ACO_REL)
4. Composed TOE testing (ACO_CTT)
5. Composition vulnerability analysis (ACO_VUL)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

These families are introduced to "*specify assurance requirements that are designed to provide confidence that a composed TOE will operate securely when relying upon security functionality provided by previously evaluated software, firmware or hardware components*".

In other words, the purpose of this class is to conduct a cheaper and faster evaluation of a system composed by several components that have already been evaluated.

2.1.2 Method description

2.1.2.1 Prerequisite

In any security assurance evaluation, the most important prerequisite is to make available the maximum information about the system to evaluate starting from the version of each element which composes the TOE. In doing so, the evaluator can gather reliable information regarding the whole system.

2.1.2.2 Composition model

The CC part 3 appendix presents the concept of composition used in the ACO class.

Most of the time, when a system is composed of several subsystems it is because of the need to have each subsystem communicating with one or several subsystems (of the same system) in order to perform a task. So, the services of a subsystem can be used by another subsystem. In that case, the component that provides the services is called the base component (noted as Base component-b) and the component that uses the services is called the dependant component (noted as Dependant component-a).

The ACO class aims at checking that the components of a composed TOE are integrated in a secured way as defined in the Security Target of the composed TOE. To reach that objective, all the interfaces between these components must be tested, the design of the components must be analysed and the related vulnerability analysis must be conducted.

2.1.2.3 ACO Components

2.1.2.3.1 Composition Rationale (ACO_COR)

The objective of this family is to determine the level of assurance of the base component and check if this level is high enough. There is only one assurance component in this family.

Basically, the base component assurance level must be greater or equal to the assurance level of the function of the dependent component which uses the base component.

The inputs needed are:

- A Security Target (ST) of the composed product

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- The version of the different products
- The reliance document
- The Security Targets of the products to be composed and if necessary, design details to help the understanding of the reliance document

The reliance document contains the list of the base component features required by the dependent component.

2.1.2.3.2 Development evidence (ACO-DEV)

The objective of this family is to identify and understand the base component functions used in order to check if the interface and architecture of the components are compatible. The security functions must be provided by the base component to guarantee that the dependent component can work properly. This family is composed of three assurance components which correspond to the three levels of knowledge of the components to be composed:

- ACO_DEV.1: knowledge of the base component interfaces. Each interface which is used in the composed TOE must be described.
- ACO_DEV.2: knowledge about the way the dependent component uses the base component interfaces and knowledge of the base component behaviour when its interfaces are used by the composed TOE.
- ACO_DEV.3: detailed knowledge of the dependent component subsystems and of the base component to understand their interactions.

The inputs needed are:

- A Security Target of the composed product
- The reliance document
- The design document of the components

Technically, the objective of this task is to link the dependences identified in the reliance document with the TOE Security Function Interfaces (TSFI) available in the base component. This task should let the evaluator know whether the TSFI used by the dependent component have been categorised as TSF-enforcing or not during the evaluation of the base component.

2.1.2.3.3 Reliance of dependent component (ACO_REL)

The objective of this family is to estimate the dependency level of the dependent component towards the base component. The inputs required correspond to the information that would be needed by the integrator of the dependent component with different base components. The final objective of these family requirements is to check if all the features needed by the dependent component to provide its security services have been correctly evaluated during the base component evaluation.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

The main problem here is that some base component interfaces, used by the dependent component, have not been evaluated during the base component evaluation because the services provided by these interfaces were not considered as related to security functions. There are two reasons for that to happen: either because the security function provided was not linked to a Security Functional Requirement in the base component ST, or because the interface provides a basic service which can be used by many functions, security related or not. For instance, a 'simple' function that multiplies two integers or that realises a string comparison can be critical when used in a cryptographic or authentication context in the dependent component.

This family is composed of two assurance components which correspond to the description levels of the features needed by the dependent component:

- ACO_REL.1: The services needed are described
- ACO_REL.2: The interfaces and return values are described

To perform these tasks, the CEM (Common Evaluation Methodology) informs that the evaluator needs more or less detailed information (depending on the level) about the dependent component design. The dependent component source code seems to be the most relevant information because the base component function calls can be easily identified.

2.1.2.3.4 Composed TOE testing (ACO_CTT)

This family aims at analysing the tests performed on the composed product and on the base component to make sure that:

- The composed product provides the expected services.
- The base component features, used by the dependent component, have been effectively tested by the base component creator.

The first point is covered by analysing the test plan of the composed product. The CEM says that the tasks related to the requirement ATE_FUN.1.1E (test class, functional test family) are conducted for that purpose.

The second point is covered by analysing the test plan of the base component relying on the dependencies mentioned in the reliance document that is provided in the frame of the requirements of the family ACO-REL. In both cases, CEM says that the evaluator must perform the evaluation task ATE_IND.2 (test class, independent test family) based on the test plan provided (of composed product and base component).

This family is composed of two assurance components corresponding to the rigor level of the tests:

- ACO_CTT.1: Interface testing
- ACO_CTT.2: Rigorous interface testing

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

2.1.2.3.5 Composition vulnerability analysis (ACO_VUL)

The objective of this family is to make sure that any residual vulnerability on the base component and on the dependent component is not exploitable in the composed product and in the context of its usage. This family is composed of three assurance components corresponding to the level of the vulnerability analysis conducted:

- ACO_VUL.1: Composition vulnerability review (research of public vulnerabilities on the base component, the dependent component and on the composed product)
- ACO_VUL.2: Composition vulnerability analysis (test of resistance to basic attacks)
- ACO_VUL.3: Enhanced-Basic composition vulnerability analysis (test of resistance to enhanced-basic attacks). At this level, the evaluator shall conduct penetration testing (cf. CC Part3 v3.1 rev5 - ACO_VUL.3.5E [1]).

In order to do this task, CEM indicates that the evaluator must have the list of the residual vulnerabilities detected during each component evaluation. Then the evaluator must analyse each residual vulnerability to figure out whether it is still valid in the composed product and in its context of operational usage. To do so, just the list of the residual vulnerabilities is not enough but the evaluator needs a complete description of each vulnerability.

The temporal aspect is not considered in the CEM for that family. If the previous evaluations of the base component and the dependent component have been conducted a long time ago:

- new vulnerabilities could have been detected, since the previous evaluation, with the improvement of the detection technics.
- some residual vulnerabilities could now be exploitable with the improvement of the attack technics.

2.1.2.4 Interaction between ACO families

Figure 3 explains the relations between the families of the class ACO. The arrow from ACO_REL to ACO_COR means that the results of the task carried out in the ACO_REL are inputs to the tasks in ACO_COR. The dashed arrow from ACO_CTT to ASE means that tasks in ACO_CTT use explicitly the SFR of the composed TOE.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

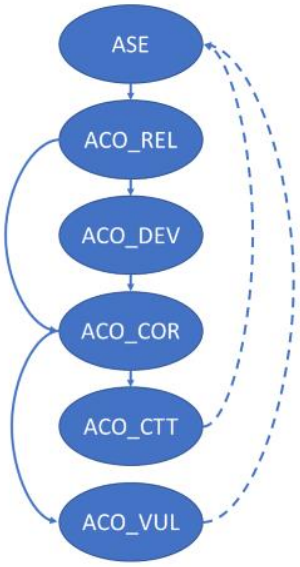

Figure 3: Interaction between ACO class families

2.1.2.5 Assurance level for composed products

Assurance class	Assurance Family	Assurance Components by CAP		
		CAP-A	CAP-B	CAP-C
Composition	ACO_COR	1	1	1
	ACO_CTT	1	2	2
	ACO_DEV	1	2	3
	ACO_REL	1	1	2
	ACO_VUL	1	2	3
Guidance documents	AGD_OPE	1	1	1
	AGD_PRE	1	1	1
Life-cycle support	ALC_CMC	1	1	1
	ALC_DEL	2	2	2
	ALC_DVS			
	ALC_FLR			
	ALC_LCD			
	ALC_TAT			
Security Target evaluation	ASE_CCL	1	1	1
	ASE_ECD	1	1	1
	ASE_INT	1	1	1
	ASE_OBJ	1	2	2
	ASE_REQ	1	2	2
	ASE_SPD		1	1
	ASE_TSS	1	1	1

Table 2: Assurance level for composed products

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Table 2 defines the different assurance components required for each assurance component CAP-level.

2.1.3 Method usage

Until today, no composition based on the requirements of the ACO class has been realised.

- People believe that using two certified products together doesn't require a new certification.
- The time and the cost of the ACO class application discourage the execution of the composition certification.
- The frame of the ACO class application is very strict and, in practice, two products which are integrated together depend on each other; whereas the ACO class requires one base product and a dependent product and the base product not to be dependent from the dependent product. This limits greatly the field of application of the ACO class.

2.2 General best practices

For systems with a level of complexity too high to be efficiently evaluated, security assurance approaches do not scale. Actually, most systems are a composition of hardware, Operating Systems, networks and application services that cannot be evaluated in detail as being one single entity. Their global security properties are natural compositions of their individual components' security properties and configurations (firewalls, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), anti-viruses, network configurations, cryptographic mechanisms, etc.).

Security in that case is generally assessed at the system-level either by doing vulnerability tests on the complete system or by doing a top-down security analysis approach. Actually, in many cases even vulnerability tests do not scale and do not provide enough evidence of security properties fulfilment. Best practices such as ISO 2700X series or information security guidelines[1] are applied to sensitive systems for which security management and demonstration are critical and are the following:

- Perform a risk analysis to
    - Identify critical system elements
        - Assets to be protected
        - Architecture components either providing security or to be protected
    - Define unwanted events to be prevented in order to protect the system correctly
    - Evaluate the associated risks
    - For the risks to be treated, define security objectives and countermeasures to be assessed
- Projection of the global requirements on local architecture elements

[1] For example https://www.ssi.gouv.fr/en/guide/40-essential-measures-for-a-healthy-network/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- For each identified local countermeasure
  - Evaluate them
    - Documentations, configuration, functional tests, vulnerability tests, etc.
  - Evaluate their interactions (composition) with the rest of the system
    - Mainly functional tests and some additional vulnerability tests when possible

The composite evaluation assurance is then provided by the risk analysis that helps define the targeted requirements at system-level and their associated projections on the local equipment. This is completed by local verification of the projections of these global security requirements.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

3 Composite Evaluation implementation in SAFERtec project

The composite assurance approach provided by SAFERtec actually re-uses the main concept of the general best practices approach:

- We have performed a global risk analysis in D2.3
- We have identified system-level security requirements in D2.4
- We have projected those global requirements onto the critical system's components to define appropriate local security requirements to fulfil global security objectives in SAFERtec Protection Profile (D3.2)
- We have proposed an assurance approach to:
    - Validate locally the security requirements in D3.3
    - Validate a composition assurance in D5.2 and D5.3 to verify the correct integration of the strong local security properties in the system. Moreover, an Assurance class AOP has been defined by SAF in D3.1

3.1 Risk analysis of SAFERtec system

For the purpose of assessing cyber-security risks on the selected use cases, the SAFERtec project developed a methodology that enables an effective consideration of all security aspects for the designed architectures. More specifically the integrated SAFERtec methodology was used for a) identifying the main assets (hardware, software, data, communication links) of the Connected Vehicle and V2X systems; b) eliciting the security, safety and privacy requirements; c) identifying threats and vulnerabilities and finally d) producing the threat and attack models of the system that is studied. The proposed methodology was based on an innovative combination of three well-known methods, EBIOS [3], SecureTropos [4] and PriS [5].

The goal was to design a methodology that helps to get from the system description and threats knowledge a detailed, clearly justified and well-structured set of security requirements for components. EBIOS is a very good tool to start the study by applying a top-down approach and to help the methodology user by guiding him to define the system and its security objectives. Then, in EBIOS, these inputs are used to derive "formally" the adequate security requirements for the different element of the system. Also, PriS provides an extra focus on privacy which is a very important topic in the field of ITS security, since we do not want vehicles to be trackable by anyone in the world. The proposed approach assists engineers in both the attack modelling and vulnerability analysis through the application of a six stages process, as presented in Figure 4 and served as input to SAFERtec publications [6], [7].

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

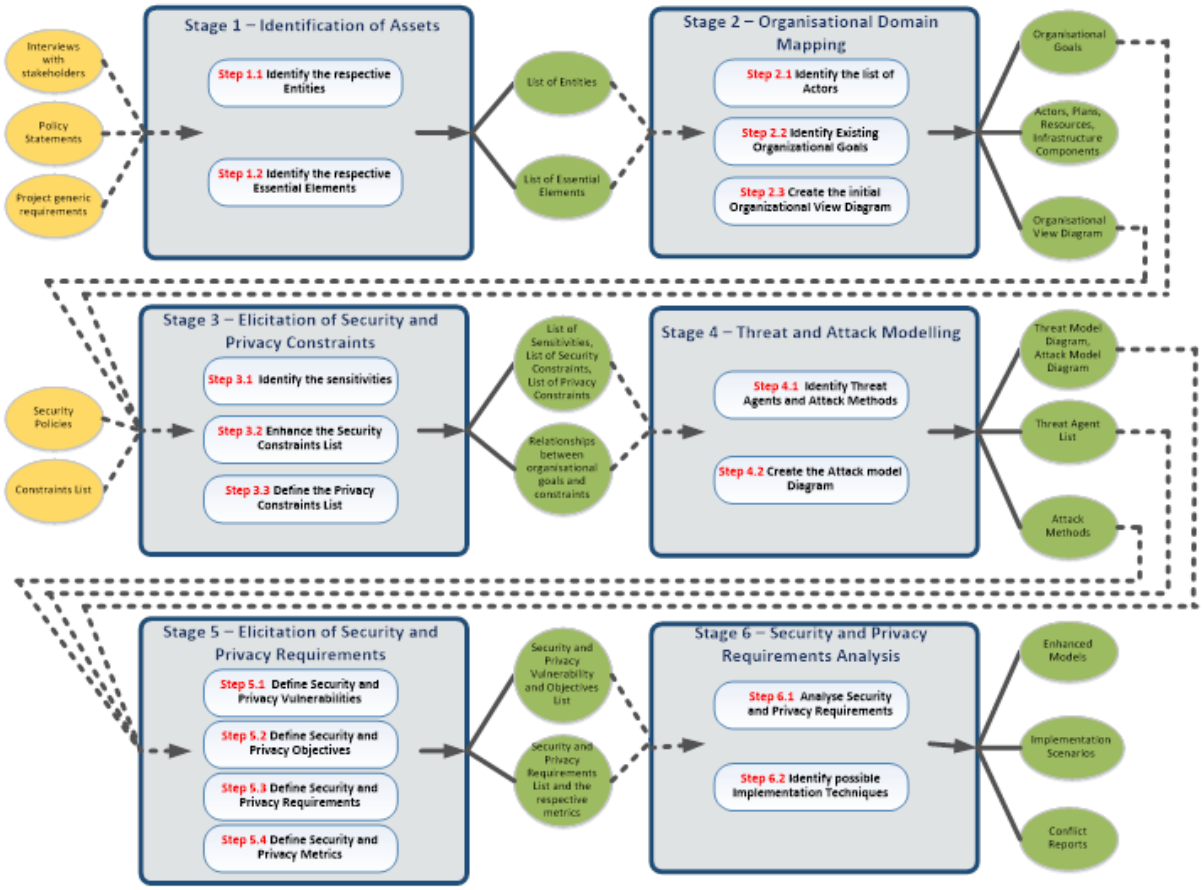

Figure 4: SAFERtec Attack Modelling Process

Specifically, in stage 1 of the Figure 4: SAFERtec Attack Modelling Process, EBIOS is introduced in order to proceed with the identification of the respective entities that correspond to the main players of the considered system. In parallel with the significant entities, the essential elements are identified. Essential elements play a key role in the threat and attack modelling process since they represent functions and information, providing added value to the entities. Entities and the respective essential elements provide the first mapping of the considered system. The steps applied in this stage are Step 1.1 Identification of the respective Entities and Step 1.2 Identification of the respective Essential Elements (see Figure 4).

In stage 2, the main effort is to understand the current organisational structure and, based on the identification of the entities and the essential elements from stage 1, to identify entities like actors, organisational goals, plans, resources, services and infrastructure. This leads to an efficient organisational analysis (in our case, an efficient mapping of every use case) which is a mandatory prerequisite for the threat and attack modelling activities in the following steps. The steps applied in

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

this stage are Step 2.1 Identify the list of Actors, Step 2.2 Identify Existing Organisational Goals and Step 2.3 Create the initial Organisational View Diagram.

In stage 3, the identification of security and privacy constraints related to the organisational needs are identified. Security and privacy needs are identified based on the security and privacy concerns that the organisation has (in our case the connected vehicle and the relevant eco-system). Thus, it is important to identify, initially, the security concerns of the organisation and understand their linkage with the identified organisational goals. Identification of sensitivities provides the first set of candidate security and privacy concerns per use case. Then, through Secure Tropos and PriS, the refinement of the sensitivities occurs considering the rest of the identified entities from the previous steps, while the list of security and privacy constraints is provided as output. These constraints should be fulfilled along with every identified functional requirement. The steps applied in this stage are Step 3.1 Identify the sensitivities, Step 3.2 Enhance the Security Constraints List and Step 3.3 Define the Privacy Constraint List (see Figure 4).

In stage 4, the threat analysis is performed following the EBIOS process along with the methodology of the ETSI standard (described in section 4 of D2.2). During this stage, the identification of every threat per organisational goal is conducted. Threat elicitation is of vital importance for capturing the external and internal sources that can cause harm to the assets of the system, but also for validating that the identified security and privacy constraints list is complete. Attack models will also be constructed for every identified threat per security and privacy constraint for every functional goal (organisational goal). Upon the completion of the specific step, the Threat and Attack Models are constructed, representing all necessary knowledge in order to be combined with the vulnerability analysis and security and privacy requirements elicitation of the following step. The steps applied in this stage are Step 4.1 Identify Threat Agents and Attack Methods and Step 4.2 Create the Attack model Diagram (see Figure 4).

In stage 5, the vulnerability analysis is conducted based on the identified threats and attack methods. Security and Privacy vulnerabilities detection leads to the identification of the security and privacy objectives, which are the way that vulnerabilities are mitigated, thus reducing the potential risk on the identified entities. The next step of the same stage is the definition of the security and privacy requirements that basically describe in a specific way the realisation of the identified objectives. This step is critical since the security and privacy requirements list will need to satisfy the identified objectives in accordance with the security and privacy constraints list and the attack models described above. Finally, in the cases were measurable indexes can be established for examining the efficient implementation of the security or privacy requirements along with other parameters (e.g., safety) are used to contribute to the identification of the proper metrics for every security and privacy requirement. The steps applied in this stage are Step 5.1 Define Security and Privacy Vulnerabilities, Step 5.2 Define Security and Privacy Objectives, Step 5.3 Define Security and Privacy Requirements and Step 5.4 Define Security and Privacy Metrics (see Figure 4).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Finally, in stage 6 the security and privacy requirements analysis is conducted. The specific stage is of vital importance since all the information collected from the previous stages are modelled under a unified model in order to proceed in the identification of possible conflicts among security and privacy, threat mitigation and vulnerability satisfaction, etc. Also, the identification of possible implementation scenarios for every security and privacy requirement is realised in order for the stakeholders and the developers to select the most appropriate solution per use case. The steps applied in this stage are Step 6.1 Analyse Security and Privacy Requirements and Step 6.2 Identify possible Implementation Techniques.

As an initial mean of threat elicitation and identification of essential assets of the SAFERtec project the ETSI Threat, Vulnerability, Risk Analysis (TVRA) [8] was used. The threat elicitation has been conducted in all SAFERtec use cases in order to enable the identification of the following specific concepts per use case. The following concepts were derived from ETSI terminology:

- Threats
- Attacks
- Targets Of Evaluation
- System Assets (Functional and Data) for the main ITS components
- Security Objectives
- Privacy Objectives
- Reliability Objectives

ETSI could not support the detailed elicitation process. However, it was a valuable source of information for specific types of data for every use case and a valuable method for feeding the initial steps of the attack modelling method.

Following the proposed methodology, the vulnerability analysis was conducted by leading to the identification and modelling of all respective security, privacy and safety requirements for every use case of the SAFERtec project. The output of the analysis was used to identify security measures and controls acting as input for the implementation of the SAFERtec Protection Profile (PP). In total 88 security and privacy requirements were analysed and modelled in parallel with the proposed safety and functional requirements of the SAFERtec project. The way that such a detailed risk analysis at system-level is projected at module-level for the vulnerabilities' identification and thus serves the needs of the SAFERtec-proposed composite evaluation, will be discussed in the following sections (mainly in 3.3).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

3.2 Security objectives and requirements per components

All investigations performed in the course of the SAFERtec project indicated that the implemented assurance framework should rely on the most common, generally accepted, well-defined, well-tested and validated assurance methodology, i.e. the Common Criteria. CC assurance is based on the definition of a protection profile (PP), thus one of the main implementation activities for the SAFERtec project is to define, determine, implement and evaluate the Connected Vehicle PP.

The objectives of the SAFERtec PP definition, the reference for the security assurance, are the following:

- The determination of the assurance-related functional components of the Connected Vehicle.
- The identification of all Connected Vehicle (cyber-physical system and network interfaces) system assets with the necessary security services
- The PP should be used to provide assurance coverage for both system and component level.
- The definition of a generic PP, that is applicable to the vast majority of modern Connected Vehicle (supporting at least 1.5 Day ITS services), as an implementation-independent architectural description. Nevertheless, effort was spent in order to design a substantially specific PP that offers real assurance for various configurations.
- Fitting of the configuration with the functional descriptions provided by ETSI in the Threat, Vulnerability, Risk Analysis (TVRA) document [8].
- Extraction of rules and methodology that can help developers and evaluators to match the actual hardware and software modules of the real system with the functional and data assets described by the PP.
- The Conformance of the Security Functional Requirements defined into the PP with standards, polices and common practices, as well as the description of application notes with recommendations for basic testing and evaluation, when possible.

The complete end-to-end analysis of the security objectives, services and requirements of the Connected Vehicle is a cumbersome activity, since the IT infrastructure of the vehicle is composed by a large set of heterogeneous hardware and software components – in most cases manufactured by various different OEMs. This fact makes it difficult to achieve the objective of the generic yet effective PP. As a solution, SAFERtec designed and implemented a modular PP [9] with the definition of objectives, controls and features for each system high-level asset or module. The concept of the modular PP helps apply the assurance procedure to various configurations from various OEMs implementing a plethora of hardware components and software of the Connected Vehicle.

For all modules and high-level assets of the modular PP, the security requirements and controls related to system reliability, safety, security and privacy are defined. Emphasis was given in the dependability and interaction among various radio/network/physical/application modules.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

In SAFERtec, the Target Of Evaluation is the Vehicle ITS Station (V-ITS-S) that includes all the functional and data assets of the Connected Vehicle. This is also a major differentiation of the SAFERtec approach from similar works targeting only the network components. The V-ITS-S is composed by all hardware, software, networking and communication components that implement all ITS services and applications for the vehicle and the passengers. It can be easily understood, that the TOE is not a single device or a specific architecture, but a set of heterogeneous physical and logical components combined in various ways in order to produce or consume data originating by various different sources - in-vehicle or through cooperative communications. The objective of the TOE is to provide secure ITS:

- From communication interfaces with other vehicles,
- From communication interfaces with the infrastructure or remote internet services,
- From elements and applications operating inside the vehicle (e.g. sensors, applications, vehicle control modules and more).

The investigations conducted by the SAFERtec project indicated that there is no common or standardized policy on the design and management of the vehicle ICT devices and services. The modular approach however, extends the applicability of the PP and the assurance framework to various architectures. The benefits introduced by the modularity of the PP are the following:

- Extensibility of the PP: New components and features can be introduced into the PP without the need to structurally redesign and redefine the PP. Only affected assets/modules will be reviewed and modified.
- Extensibility to other relevant systems: The modular PP concepts (as well as the PP modules) can be reused for the formation of PPs for other relevant systems, e.g. roadside units.
- Upgradability: new modules can be attached to the Protection Profile without the need for a structural redefinition of the complete system or the base PP.
- Ability to integrate: If existing validated PPs are used for subsets or subsystems of the V-ITS-S, then they can be seamlessly integrated into the assurance framework as modules of the PP. This has already happened for the Hardware Security Module (HSM), where a PP accepted by the car industry already exists [10]. In this case, there is no need to perform redundant actions or review the complete profile. It is sufficient to review the base PP in order to define proper interfaces and roles and define some new configurations that contain the added module.
- Wider Acceptance: The SAFERtec project invested time and effort to propose a PP that can be applied to any investigated Connected Vehicle architecture. Nevertheless, even if it cannot fit a specific architecture as a whole, specific modules will be applicable and the evaluator or developer can use them to compose the Security Target.

In order to define a modular PP, the following logical entities (corresponding to physical and logical resources) have to be defined:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- *The base PP* that contains all system assets that are expected to be found in every possible V-ITS-S architecture and implementation. The base PP should also define interfaces and interconnections with other assets/components, called modules.
- *The PP module* that are assets of the V-ITS-S that are not mandatory for an implementation or a configuration. However, the module defines an extended attack surface and offers new functionalities and services covered from the respective PP.
- *The PP configuration* that is the result of the combination of the base PP with at least one PP module in order to constitute the investigated V-ITS-S.

The definition of the modular PP in SAFERtec has been made using the following steps:

- Review the work done in [8] to define the high-level assets of the V-ITS-S. If necessary, the model should be extended (e.g. in order to include the HSM in the model).
- The high-level assets that are considered mandatory for all V-ITS-S are unified in order to constitute the base PP.
- The high-level assets that are optional or 'mandatory optional' (for example a communication interface is necessary but it may be V2X or conventional cellular) are extracted as modules.
- Depending on the investigated architecture, the system configuration (that will result in the configuration PP) is extracted.

According to the aforementioned rationale, it was decided that:

- The base-PP includes
  - The applications
  - The V-ITS-S data assets
  - The service control subsystem that controls all in-vehicle device/system/software interaction.
- The modules are:
  - The Communication Unit(s) (or according to [8] terminology the Protocol Control).
  - The Sensor Monitor (i.e. the sensor driver/firmware/control module).
  - The Vehicle Control Monitor (i.e. the firmware/driver/control module that drives/activates vehicle components – for Day 1/1,5 applications).
  - A cryptography module, the Hardware Security Module (HSM), i.e. a secure module integrating key storage and cryptographic functions. Here, it should be noted that the HSM is considered now mandatory; however it was defined as module in order to reuse the PP defined by the Car 2 Car Communication Consortium [10].

The next step was to use the results of the work presented in Section 3.1 : the system-level risk analysis and the definition of system-level security requirements in order to derive the threats for each high-level asset (as part of the base PP) and for each module. With this step, SAF seeks to avoid

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

common composition mistakes and limitations by taking directly into account composition constraints while listing components requirements.

It is noted that based on the particularities of each asset/module different threats (or threat "flavors") may apply. Nevertheless, a superset of generic threats/attacks can be defined, that includes:

- Extreme solicitation
- Jamming
- Data manipulation
- Data leakage
- Firmware/application alteration
- Unauthorized access
- Reverse Engineering
- Sybil attack
- Address/Equipment Spoofing
- Local network attack
- Replay attacks
- Impersonation
- Illegal information inflow/outflow
- Malicious code injection

Those threats can become more specific and focused when investigated per asset/module. Thus, for example, ITS message spoofing or tampering in the Communication Unit is considered as Data Manipulation.

The aforementioned threats when implemented with specific attacks to the various system assets compromise the function of the system and its ability to provide secure services. The threats affect specific security objectives. The security objectives address the protection to be provided by the TOE. It defines a desired/necessary security state of an entity or data of the system and represents the main goal of a security policy. For each high-level asset or module, the security objectives were defined depending on possible threats, on the operational environment and some assumptions. Despite the fact that each module or asset has specific needs, security services and therefore special security objectives, a set of a generic superset of objectives can be defined, and with some specialization, and depending on the case, can be applied to all assets/modules separately. These are:

- Software Integrity
- Integrity of received (incoming) data
- Integrity of stored data
- Availability of received data
- Availability of transmitted (outgoing) data

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- Availability of stored data
- Confidentiality of transmitted data
- Confidentiality of stored data
- Unlinkability of transmitted data
- Stored data anonymity
- Authenticity of received data
- User authorization
- Isolation of stored data
- Accountability

Finally, the implemented PP for the base and each module follow the steps below:

1. The threats, together with the defined security policies and the assumptions define the security Operational Environment.
2. The security objectives for each high-level asset and module determine the overall objectives of the TOE. Together with the Operational Environment objectives, it defines the complete system security objectives.
3. Lastly, the security functional and assurance requirements are defined.

The Security Functional Requirements (SFRs) determine a set of identified security controls and measures that can protect the TOE from its environment and the imposed threats.

In SAFERtec, great effort was spent in order to implement an assurance framework based on security requirements that can secure the Connected Vehicle. The composition of SFRs is based on standards, common practices and validated security policies. However, the SAFERtec PP is a "live document" that evolves together with the TOE and the new standards and recommendations that are published. Thus, new SFRs are added in order to cover vulnerabilities from existing or new threats.

The adopted top-down approach to derive the security requirements of components allowed to project the results of the SAFERtec system-level risk analysis i.e., the (global) security requirements over the system's critical components. Thus, SAF manages to directly account for the composition constraints i.e., the relevance of the component-level security measures and their implementation to the provision of a secure system at the end.

3.3 Evaluation of security objectives per component

The evaluation of the security objectives is a constitutive part of the SAFERtec Security Assurance Framework (SAF) and is presented in deliverable D3.3.This task aims at checking that each Target of Evaluation meets its security requirements defined in Section 3.2.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

3.3.1 Preliminary tasks

The security objectives are the result of the application of several preliminary tasks which are briefly reminded here.

The risk analysis, following the new SAFERtec approach described in the chapter 3.1 Risk analysis of SAFERtec system , constitutes the first step of the application of the SAF. The result of this step is a list of risks associated to the TOE.

The second step aims at defining the Security Objectives that correspond to the risks that have been identified in the previous step.

The Security Requirements are derived from the Security Objectives. This is the third step which has been carried out during the writing of the modular Protection Profiles described in the previous chapter. The Security Target which formally defines the involved security functional requirements (SFRs) and security assurance requirements (SARs) referring to one specific TOE implementation, is obtained at the end of this step which allows to perform the security evaluation.

Figure 5 describes the different steps that have been necessary to conduct the security evaluation.

Figure 5: From the risk analysis to the vulnerability analysis

3.3.2 The Security Evaluation

The vulnerability analysis has been conducted separately on the different TOEs based on each TOE's security requirements derived from system-level risk analysis. The aim was to assess the implementation (and the efficiency) of the Security Functional Requirements on the TOE through different types of tests as penetration tests or deep-dive analysis.

Firstly, a round of penetration tests has been performed on the TOE. This round allowed to discover numerous flaws, weaknesses and misconfigurations that could have been corrected by the corresponding partners. Each problem identified has been documented with a proof of exploit (e.g. screenshot), its source and estimated levels of the involved impact, exploitability and potential risk.

Source	Impact	Exploitability	Risk
Configuration	Very high	Difficult	High

Table 3: Sample of vulnerability evaluation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Additionally, its score following the Common Vulnerability Scoring System (CVSS) [11] has been calculated. This score, which ranges from 0 to 10, is a value that considers three metrics: the base metrics, the temporal metrics and the environmental metrics.

For example, the table au-dessous displays the different base metrics and their corresponding levels.

Metrics	Levels		
Confidentiality (C)	None	Partial	Complete
	0,0	0,275	0,660
Integrity (I)	None	Partial	Complete
	0,0	0,275	0,660
Availability (A)	None	Partial	Complete
	0,0	0,275	0,660
Access Vector (AV)	Local	Adjacent network	Network
	0,395	0,646	1,0
Access Complexity (AC)	High	Medium	Low
	0,35	0,61	0,71
Authentication (Au)	Multiple	Simple	None
	0,45	0,56	0,704

Table 4: The CVSS Base metrics

This first round of evaluations allowed to highlight that some SFRs were not fully implemented by partners.

Following this, a deep dive analysis of the V2X On Board Unit has been conducted with the black box approach having the same objective in mind: check locally the implementation of the SFRs. In this approach, no information was given to the auditors so they can take the place of real attackers.

Given the time and budget constraints, this analysis has been performed on the project only on a set of relevant and representative Connected Vehicle System elements such as the V2X On Board Unit modules and more specifically on the OBU ITS application, the OBU HSM and the OBU protocol control.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

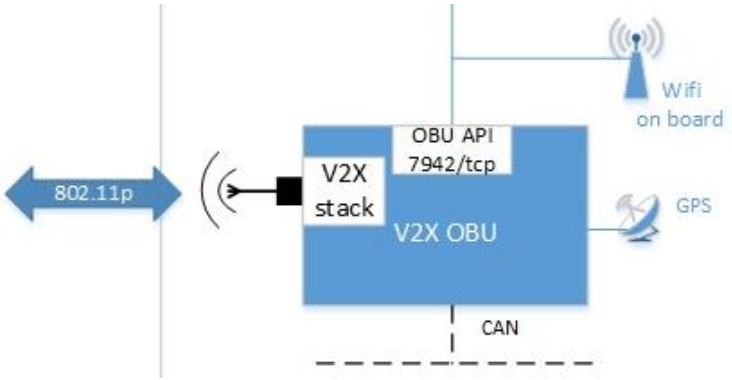

Figure 6: The considered V2X OBU and relevant interfaces

The focus has been made on the OBU as there are many access points on it that enlarge the attack surface. In this deep dive analysis multiple techniques have been used e.g. reverse engineering to understand the functioning of a component and discover the possible entry points or fuzzing tests to evaluate the behaviour of a device and the associated software.

Each vulnerability has also been documented with a real attack scenario, its prerequisites, impact and related vulnerabilities, if relevant, providing each time a proof of exploitation. A score following the CVSS has also been calculated to estimate a security level as objective as possible.

3.3.3 Results of the vulnerability analysis

Several vulnerabilities have been discovered in the first round of penetration tests and in the deep dive analysis that followed. Those results were confidentially announced to the individual SAFERtec partners who implemented the corresponding module and in certain cases further actions to improve/fix the issues, were taken. The corresponding fixes (where relevant) were validated by subsequent system-level testing (see D5.2).

Unfortunately, due to confidentiality reasons, we are not allowed to present them in this public deliverable. Further information can be found in the deliverable D3.3 which is confidential. These component level evaluations represent the first step of a bottom-up assurance validation process.

3.4 Assurance composition evaluation tasks

Some extra verifications in the final system have been done in D5.2 to assess that TOEs were correctly configured and interconnected in the 'Connected Vehicle System' developed in WP4, as specified by the STs and regarding the new assurance component we have proposed in SAF (AOP, cf D3.1). However, the final level of maturity of the complete CVS implemented in the project was not

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

high enough to meaningfully validate AOP evaluation tasks. For AOP to be relevant the whole CVS prototypes should have been close to TRL9, which was not the goal of the project.

For instance, since the identified TOEs (and their operational configuration requirements) were only partially evaluated and since not all critical elements, TOEs are interacting with, have been evaluated too, it was not relevant to study details of configuration and interactions between only partially evaluated components.

Sections 3.3 and 3.4 highlight the top-down assurance validation process put in place by SAF, starting by assessing the implementation of SFRs at component level before checking the SFRs related to the system integration in order to overcome traditional assurance composition issues. Those include (but are not limited to) the identification of non-compatible local properties or the incorrect use of evaluated functions within the system.

So, we did operational verification of the conformity of the CVS to its STs, i.e.: (i) verifications of configuration conformity to the STs, (ii) verification of operational environment assumption made in the STs (e.g. integrity verification of the TOEs, availability of critical services such as time and position, procedural verification of other services integrity and trustworthiness).

3.5 Vulnerability tests on SAFERtec system for composition validation

Finally, to more concretely evaluate SAF relevance for assurance composition, we have reused work done in other WP5 tasks since the SAF has already been tested by different partners with multiple techniques as reported in D5.2 and D5.3 (vulnerability tests to evaluate resilience to real attacks). Those system-level tests correspond to the validation of the full SAF approach on the 'Connected Vehicle System' (CVS) and the extended modules, namely modules that were originally developed in the context of WP4 (and subsequently extended as suggested by the SAF application: HMI user authentication feature and the V2X misbehaviour detection layer).

In the current deliverable, we do not run any further tests but provide a new analysis of the evidences already produced taking the assurance composition and its validation as a new point of view.

In the same way, as proposed for the component level validation of SAF, we used the attack simulation done in T5.2 to validate the composite approach or identify potential assurance composition problems (or limitations). To do that we analysed vulnerabilities that could demonstrate weaknesses in the SAF assurance composition, that are vulnerabilities which allow to bypass evaluated SFR (security functions evaluated on one of the evaluated TOEs in T3.3) on the different TOEs. A typical example would be two TOEs for which we respectively evaluated signature generation and verification mechanisms, but in the final operational system an attacker intercepting messages manages to modify the signed content and the receiver (due to bad configuration) accepts the message even though it did not validate the signature. This can happen since often security

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

mechanisms can be disabled to ease users or admin experience. Another example could be an attacker connected to a weakly configured equipment (e.g. default or easily guessable admin password) and who is from there able to connect to an unprotected interface of one of the evaluated component whose evaluation made the assumption that this interface was not accessible by unauthorized users.

The tests results used as inputs of this study have already been classified a first time in D5.3 as either:

- TOEs vulnerabilities
    - Vulnerability under SAF correction
    - Outside the TOE (ST) boundaries
- Vulnerabilities for none TOEs equipment

The first subcategory 'Vulnerability under SAF correction' (e.g. OBU Out-of-date kernels missing latest security fixes or Root accounts used for direct logins) is not to be taken into account since those vulnerabilities have to disappear thanks to SAF.

The second subcategory 'Outside the TOE (ST) boundaries' demonstrates some limitations, but they have to be considered not as assurance composition limits but as risk analysis required updates. And SAF already handles this as demonstrated in D5.3.

In fact, the last category is the one that provides further evidence on the appropriateness of our assurance composition approach as these vulnerabilities are the ones that allow to identify composition weaknesses.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

4 The SAFERtec Assurance composition evaluation analysis

4.1 Final assurance provided

At the moment of writing this deliverable and regarding project implementations limitations as discussed in section 3.5 and 4.2, the SAFERtec partners have identified no issues, neither in the SAF framework definition (feasibility) nor witnessed evidences that SAF does not provide assurance composition.

When analysing vulnerabilities identified in D5.2 and D5.3 deliverables (where auditors simulated real attacks), partners identified that they were mostly due to a partial implementation of SFRs at component level and so were identified in D3.3, by the SAF evaluation at component level, and were under correction process.

The rest of the observed vulnerabilities were related to the TOEs environment, i.e. none evaluated CVS components as the RSU, the network gateway, the OSs running the TOEs…

More precisely, the following vulnerabilities have been found:

- On the network router:
  - Use of unmaintained or out-of-date software
  - Clear text submission of password during authentication
  - Root accounts used for direct logins
  - Network resources are not properly isolated
- On the roadside unit:
  - Out-of-date kernels missing latest security fixes
  - Root accounts used for direct logins
  - Presence of services running with administrative privileges
  - Presence of sensitive world-readable files
  - Presence of guessable system passwords
  - Network resources are not properly isolated

After analysis, we have concluded that none of those vulnerabilities have been identified in the composition (interaction link) of two evaluated functions. Also, none of those vulnerabilities could be exploited to bypass evaluated mechanisms. For instance, the vulnerabilities found in the network did not allow us (regarding the project tests resources and the chosen attacker level) to be used to tamper protected data integrity.

Moreover the composition of the evaluated data integrity protection mechanisms (HSM signature function, V2X OBU information flow control function and the SAFERtec AppOBU user data protection function) could not be bypassed by the other (sometimes important) vulnerabilities despite their great number.

So this highlights that the top-down approach used for the security requirement definition followed by the bottom-up approach for the assurance validation, ensures the efficiency of the SAF assurance composition.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

4.2 Scope and results limitation

It is essential to mention that the results presented in Section 4.1 are limited by the fact that all the critical components of the 'Connected Vehicle System' specified and developed in the WP4 have not been fully evaluated in T3.3 and that some identified anomalies were not early-enough fixed to allow more comprehensive evaluations.

Also, partners did not manage to fully run the SAF (newly defined) assurance composition class (AOP) that should have provided even more assurance at system level. As proposed by SAF (cf D3.1) the composite evaluation requires operational evaluation that is in-practice dependent on the product's TRL (which was in our case far from a commercial product) and on the full evaluation of the independent components.

The SAF theoretic proposal for composite evaluation points to the exhaustive testing of the identified SFRs; in our case this was beyond the project experimentation capabilities (as more than 120 SFRs were originally identified in the SAFERtec PPs).

All above means that potential issues that we might not have identified could exist either because we did not have the resources to fully evaluate the composition or because of a flaw in our approach. Thus, we were not fully able to demonstrate by real example SAF assurance composition efficiency.

Nevertheless, the first evidences we provided are good and demonstrate at least partial efficiency. It is important to note that our theoretic contributions to the composite evaluation retain its value while our observations and testing results already provided a partial view of the final SAF composition result. More concrete technical feedback should be generated and used to further validate our approach. Our overall conclusion in this context is that we did identify no issue, neither in our framework nor in our first theoretical analysis, but more exhaustive studies (beyond the scope/limitations of a research project) should be done to fully demonstrate the SAF composition approach benefits.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

5 Conclusions

A global security evaluation is difficult especially for such systems as the Connected Vehicle System composed of several complex sub-systems. For such systems one tends to rely on already evaluated sub-systems, but this may not be enough to provide solid assurance arguments at system-level. In fact, the evaluation at sub-system level may occasionally become useless as it provides a false sense of assurance if the evaluated sub-systems are not used correctly.

In this deliverable we have first studied the assurance composition state-of-the-art which is mainly restricted to the Common Criteria class ACO (for Assurance Composition). Although it is the so-far only available approach, it has rarely been successfully applied, mainly due to its strict constraints that do not cope with practical needs. To overcome the limitation and provide more efficient assurance composition, we rely on best practices captured by our evaluation experiences to introduce the SAFERtec composite (i.e., system-level) evaluation approach.

Our proposal, represented as a V-shape assurance activity, includes first a top-down requirement definition approach that starts from the comprehensive SAFERtec system-level risk analysis, the SAFERtec modular PP and reaches up to the identification of security requirements for the connected vehicle critical components. We thus, map the identified system requirements over the components to be evaluated accounting for the composition constraints i.e., the local dependencies/interactions that security controls may have. Then, the second part (of the V-shape) includes a bottom-up assurance validation process of increasing scope validation processes aiming to first assess locally the assurance that each individual component meets its requirement and then, validate the full system security capacities thanks to extra verification of the integrated operational CVS outperforming traditional assurance composition approaches.

To validate the proposal, the SAF has been repeatedly tested over the complete ‘Connected Vehicle System’. The system-level testing has been considered from a composition validation standpoint aiming to provide experimental evidence that no composition weaknesses can be identified given an earlier obtained local assurance (even if individual components were not fully evaluated).

We do acknowledge that our results are limited by the fact that not all CVS critical components were validated by the SAF while the included new assurance composition class (AOP) was not exhaustively applied due to resources limitations (multiple iterations are needed). However, our preliminary results are very promising suggesting that the SAFERtec (V-shape) approach can provide more assurance at system-level. The expectation and worthy ambition are that further technical feedbacks will more clearly reveal the SAF composite evaluation effectiveness and render the SAFERtec framework the dominant choice in automotive security assurance evaluations.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 732319

6 References

[1] Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components – April 2017 - Version 3.1 - Revision 5 https://www.commoncriteriaportal.org/cc/

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5 https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf

[3] ANSSI, EBIOS – expression des besoins et identification des objectifs de sécurité : https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

[4] Tropos, Security : http://www.troposproject.eu/node/301

[5] Christos Kalloniatis, PriS Methodology: Incorporating Privacy Requirements into the System Design Process : https://www.academia.edu/2845236/PriS_Methodology_Incorporating_Privacy_Requirements_into_the_System_Design_Process

[6] Chr. Kalloniatis, V. Diamantopoulou, K. Kotis, Chr. Lyvas, K. Maliatsos, M. Gay, A. Kanatas, C. Lambrinoudakis, *Towards the design of an assurance framework for increasing security and privacy in Connected Vehicles*, International Journal of Internet of Things and Cyber-Assurance, 2019. Id. number: IJITCA-22922

[7] Vasiliki Diamantopoulou, Christos Kalloniatis, Christos Lyvas, Konstantinos Maliatsos, Matthieu Gay, Athanasios Kanatas, Costas Lambrinoudakis, “Aligning the Concepts of Risk, Security and Privacy towards the design of Secure Intelligent Transport Systems”, The 23rd Euro Working Group of Transportation Meeting, Paphos, Cyprus, 16th-18 September 2020 [submitted].

[8] ETSI TR 102 893 V1.2.1 (2017-03) Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA).

[9] K. Maliatsos, C. Lyvas, P. Pantazopoulos, C. Lambrinoudakis, A. Kanatas, M. Gay, and A. Amditis. 2019. Standardizing Security Evaluation Criteria for Connected Vehicles: A Modular Protection Profile. In 2019 IEEE Conference on Standards for Communications and Networking (CSCN). 1–7.

[10] Protection Profile V2X HSM CAR 2 CAR Communication Consortium – Working Group Security (WG SEC).

[11] First, Common Vulnerability Scoring System SIG : https://www.first.org/cvss/

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 732319