D6.3 –Assurance Framework Toolkit Prototype [DEMO DOCUMENTATION]

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:	**D6.3 Assurance Framework Toolkit Prototype**
Work package:	WP6
Due Date:	31 March 2020
Dissemination Level:	PU
Deliverable Type:	DEM

Authoring and review process information	
EDITOR Angelos Stamou / ICCS	**DATE** 05-03-2020 – 30-04-2020 – 24-07-2020
CONTRIBUTORS Panagiotis Pantazopoulos / ICCS Konstantinos Maliatsos / UPRC Guillemette Massot / CCS	**DATE** 04-05-2020 – 27-07-2020 29-04-2020 30-04-2020
REVIEWED BY Sammy Haddad / Oppida Claudio Griglione / Swarco	**DATE** 04-05-2020 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	07/04/2020	ICCS	First draft
V0.2	16/04/2020	ICCS	Section 1
V0.3	22/04/2020	ICCS	Section 2 and Conclusions
V0.4	29/04/2020	ICCS	Executive Summary and Refinements
V0.5	04/05/2020	Oppida	Internal Review
V0.6	04/05/2020	Swarco	Internal Review
V1.0	05/05/2020	ICCS	Final Version

V1.1	22/07/2020	ICCS	Revised to include:
			• An introductory paragraph explaining and justifying the framework's changes and relevant implications (Section 1, second paragraph).
			• A clarification of the (two) AFT interfaces (Section 2, first paragraph)
			• Comments on the updates made in the video demonstrator (which constitutes the SAFERtec D6.3)
			  o Description of the problems the AFT solves and its intended users (Section 2.1, Section 2.5 and the new Section 3)
			  o A potential practical usage of AFT (Section 2.2)

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

Table of Contents

Acronyms and abbreviations 5

Executive Summary 6

1 Introduction 7

1.1 Purpose of the Document 8

1.2 Intended readership 8

1.3 Inputs from other projects 8

1.4 Relationship with other SAFERtec deliverables 8

2 Demo Storyboard 9

2.1 First part: demo introduction 9

2.2 Second part: AFT usage example and data entry 10

2.3 Third part: ST compilation (ASE evaluation class) 11

2.4 Fourth part: ToE functional description (ADV evaluation class) 12

2.5 Fifth part: closing the demo 12

3 Challenges addressed by AFT and potential users 14

4 Conclusions 15

References 16

List of Figures

Figure 1 The introductory sequence of frames of the first part 9

Figure 2 The video frame presenting a potential use-case of AFT 10

Figure 3 The AFT current knowledge base shown in the video second part 11

Figure 4 The first frame of the third part 11

Figure 5 The AFT graphical tool (ADV class) shown in the fourth part 12

Figure 6 The AFT frame describing in-brief its potential users 13

Figure 7 The video closing frame 13

Acronyms and abbreviations

Abbreviation	Description
ADV	Development (CC evaluation class acronym)
AFT	Assurance Framework Toolkit
ASE	Security Target Evaluation (CC evaluation class acronym)
ATE	Tests (CC evaluation class acronym)
CC	Common Criteria
EC	European Commission
GUI	Graphical User Interface
OEM	Original Equipment Manufacturer
PP	Protection Profile
SFR	Security Functional Requirements
SPA	Single Page Application
ST	Security Target
ToE	Target of Evaluation
UI	User-interface

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 SAFERtec Assurance Framework Toolkit has been described in D6.1 in terms of its architectural design and in D6.2 in terms of implementation. The final deliverable of WP6 is a video demonstrator that showcases the functionality realized by the toolkit.

The document at-hand accompanies the video providing a short description of the demonstrator aiming to facilitate the viewers' better understanding.

The AFT is to the best of our knowledge the only platform-independent open-source on-line toolkit build to support CC-based evaluations and with the video circulation is expected to gain further visibility within the community of security evaluation experts.

1 Introduction

The SAFERtec security assurance framework relies on the most credible and Internationally recognised security assurance standard, the Common Criteria (ISO/IEC 15408). The need for the highest possible assurance posed by the ever-increasing automation of the connected vehicles mainly justifies this choice.

The considered standard and accordingly the SAFERtec proposal (introduced in WP3) suggest a rich spectrum of evaluation tasks over the evaluated system (i.e., Target of Evaluation). SAFERtec considerably enhances the Common Criteria (CC) introducing a tailor-made framework of *direct* and *cost-efficient* applicability to the connected vehicles paradigm. The Common Criteria processes are therefore respected; for instance, the assurance level of any evaluation is not 'computable' but predefined by the standard, essentially determined by the depth of the evaluation tasks the standard suggests. At the same time, carefully designed contributions aim to ensure the cost-efficiency of the SAFERtec proposal. AFT serves this purpose by providing the necessary online functionality to ease the gathering, organization, management of SAFERtec (or CC) evaluation data as well as the efficient compilation of the relevant outputs (e.g., Security Targets, Architecture specifications of the ToE). Accordingly, all AFT software modules (e.g., knowledge base) have been designed and developed to meet the relevant requirements (see D6.1 and D6.2).

To demonstrate the operation and supported functionalities of a software is not straightforward. Any effort needs to be characterized by clarity, easy-to-follow presentation and attractiveness. To serve those purposes we have chosen to produce a video demonstrator that will showcase the AFT capabilities. Furthermore, a video file can be easily circulated and act as an effective 'promoter' both of the AFT advantages and the entire body of the SAFERtec work. A more technical note relates to the AFT implementation as a SPA; the approach of bringing all functionalities to the user through a single page can be very well captured by video frames.

A video of around 3:50 minutes long has been carefully designed and compiled to summarize the AFT capabilities. Its duration seeks to strike a balance between the sufficient provision of information and the long duration that may cause frustration. The demo video is enriched with subtitles (i.e., informative messages over most of its parts) that seek to provide explanations of what is -at each moment- shown.

In what follows we describe the five main (logical) parts of the demo video discussing how the implemented functionality is showcased. The video file (when approved) will be uploaded in the SAFERtec webpage to facilitate the project outcomes' dissemination while the toolkit source-code is already available for free download [1] from interested audiences.

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

1.1 Purpose of the Document

This is a short document briefly describing the high-level storyboard of the video made to showcase the AFT functionality.

1.2 Intended readership

Besides the project reviewers, this document is addressed to any interested viewer of the AFT demo video (*i.e.*, Public dissemination level).

1.3 Inputs from other projects

No inputs from other projects have been used to this document editing.

1.4 Relationship with other SAFERtec deliverables

This document complements the AFT video demonstrator. The relevant software design work of the presented toolkit relates to D6.1 and the corresponding implementation to D6.2.

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

2 Demo Storyboard

The demo video is conceptually 'divided' into five parts: the introduction screen(s), the data entry part, the part related to the ST (i.e., ADV assurance class), the part related to the description the ToE functional specifications (i.e., ADV assurance class) and finally the outro screens(s). Note that the specification of the tests (ATE assurance class) is not shown as the relevant functionality has been identified as a possible future extension (see D6.3).

One final remark relates to the presented point-of-view and the relevant AFT user-interfaces (see D6.1). AFT has been designed with two user (role) interfaces: one to recognize and support the certified expert user allowing for full access to the AFT knowledge base (with edit rights). The second one supports the typical user and allow him to operate the toolkit, retrieve information and prepare the evaluation input data required for security assurance evaluation of automotive products. For the sake of efficiency those two interfaces were developed in unison in order to support users of both roles, simplify deployment, reuse components and promote user friendliness. In another case, for instance, an expert user would need to log-in/log-out from the second interface and then log-in again to the first one. The AFT video demonstrator presents snapshots of a user with both roles enabled in order to showcase the full functionality.

2.1 First part: demo introduction

This part lasts for about 35 seconds. It familiarizes the viewer with the SAFERtec logo and provides a sequence of short textual notes (see Figure 1) on a) the challenge that SAFERtec addresses; b) the approach that SAFERtec adopts and the involved resources requirements and c) the AFT functionality (in the aforementioned context) i.e., the automated support of CC-based or SAFERtec-based security assurance evaluations.

Figure 1 The introductory sequence of frames of the first part

Then, the main UI page is shown explaining with the usage of subtitles the functionality behind each of the 4 main AFT choices (buttons):

- Entities definition
- Security Targets

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

- Functional Specifications
- Tests

Furthermore, it is shown that the first functionality involves the (security) expert user who will enter/update the data[1] in the system while all others involve the regular users i.e., the ToE developers who use AFT to efficiently gather and prepare the required inputs for a CC-based evaluation of the corresponding ToE.

2.2 Second part: AFT usage example and data entry

This part lasts for about one minute. The opening frame suggests that the following video content may stand as an example of the AFT functionality (see Figure 2). In particular, one may consider that the AFT user seeks to proceed with the CC/SAFERtec evaluation of a connected vehicle module (such as a sensor) under an automated driving use-case (e.g., Green Light Optimized Speed. Advisory). The way that AFT can assist the user towards compiling the required information (in terms of the required data entry, involved Security Target and architecture specifications) is presented in the subsequent part of the video.

Figure 2 The video frame presenting a potential use-case of AFT

For the data entry the video presents the list (i.e., knowledge base) with the already available AFT entities (see Figure 3). It is important to note that the various CC mandatory elements of the knowledge base are connected properly by enforced relationships defined by the CC standard. Those relationships are illustrated in a diagram (permanent for this page, shown in Figure 3) at the right-most corner of the AFT screen, to ease the user.

Then the video showcases the fields needed for the addition of a new one. After creating a new one (e.g., an asset) the user can associate it with other AFT entities (e.g., products and pre-defined threats) or add/edit new ones (e.g., a new threat).

[1] Note that the current AFT knowledge base has been populated using data from the SAFERtec PP [2].

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

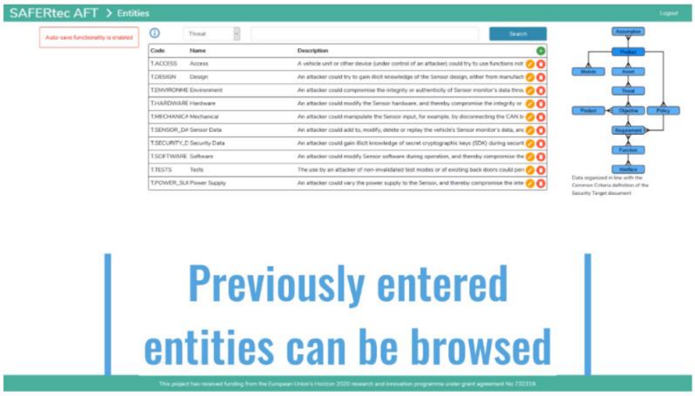

Figure 3 The AFT current knowledge base shown in the video second part

Finally, the user may navigate through the different entities inspecting also the relevant links to the different PP data entry, as defined by the CC standard (i.e., the user enjoys a direct view of the threats, assumptions, security objectives that are linked to a certain asset). A search functionality is typically supported by AFT (not shown in the demo).

2.3 Third part: ST compilation (ASE evaluation class)

This part lasts for about 43 seconds. It presents the AFT provided functionality to assist the ToE developer in the compilation of the ST. The main ST page where an overview of all ST fields as defined in CC, is presented and the viewer is notified about the capability of browsing through them (see Figure 4).

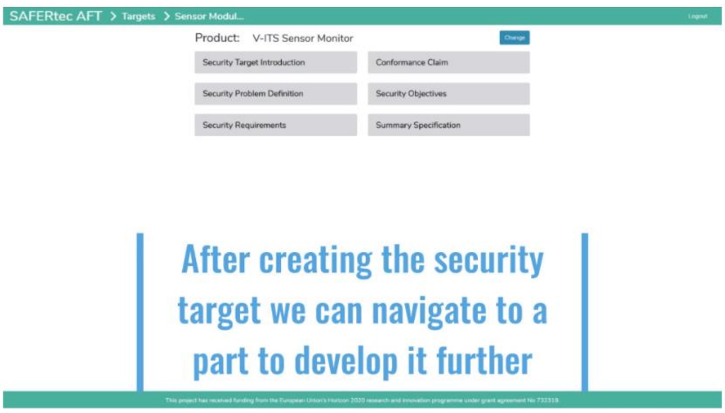

Figure 4 The first frame of the third part

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

The various placeholders for editing/storing the ST entries feature appropriate information buttons to guide the user on the needed inputs (as defined by the CC standard). Finally, the demo shows a part of the ST definition whereby the AFT user is enabled to further edit the ST field and add new threats and ST assumptions.

2.4 Fourth part: ToE functional description (ADV evaluation class)

This part lasts for about 25 seconds. The AFT provides a GUI (see Figure 5) to assist the user (i.e., ToE developer) in providing a clear description of the ToE design in terms of functional specifications. The user can select different 'shapes' that represent already defined entities, assets or ToE modules from the panel of the graphical environment. Various connections can then provide links in-between marking the correlation of each link (representing ToE interfaces) with the ToE security functions and already identified SFRs (coming from the corresponding ST).

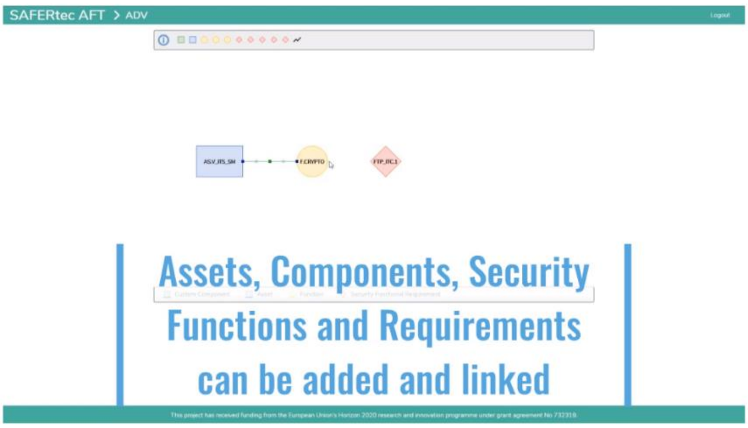

Figure 5 The AFT graphical tool (ADV class) shown in the fourth part

2.5 Fifth part: closing the demo

This part lasts for about 25 seconds. It provides a short outro starting with a brief note on the toolkit's potential users (see Figure 6). More details are provided in Section 3 of this document.

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

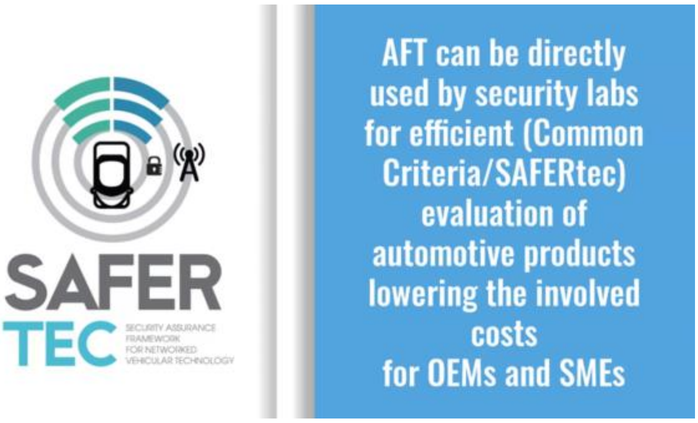

Figure 6 The AFT frame describing in-brief its potential users

Next, it provides links to the SAFERtec webpage and the git page where the AFT source code has been uploaded and freely provided to any interested party [1]. ICCS is mentioned as the AFT designer and developer while in the last frame (see Figure 7) the logos of all consortium partners together with the acknowledgement to the EC funding are shown.

Figure 7 The video closing frame

3 Challenges addressed by AFT and potential users

The introduced SAFERtec security assurance framework seeks to provide the means to increase the effectiveness of the evaluation of current cyber-security solutions (trying to assess the confidence that this technology meets the relevant requirements).

Achieving the highest (possible) levels of assurance for a security evaluation such as the one provided by the Common Criteria standard that SAFERtec relies-upon, implies a comprehensive description of security requirements and execution of an exhaustive list of evaluation activities. It follows that the involved costs[2] are increased (compared to other approaches of lower assurance), hindering the applicability of the approach; especially over complex products such as the connected comprising the connected vehicles ecosystem.

Two are the main means to reduce costs; one is to adapt the Common Criteria framework and its needs to a certain domain (e.g., the automotive ecosystem) while the second and presumably most effective one, is to introduce dedicated to that domain, software tools that propose default values and help gathering the required input-data, automating the evaluation. The carefully design of the SAFERtec framework relates to the former thread while the presented AFT software serves the latter purpose.

So far, to the best of our knowledge no open-source solution has been developed for the evaluation of the connected vehicles; furthermore, previous approaches that are not tailor-made for automotive usage can apply only on certain platforms or require already certified products. AFT has been designed to address those gaps.

Along this line, the AFT software is expected to be used mainly by organizations/experts that take over the task of security assurance evaluation (e.g., accredited Common Criteria evaluation labs, certification authorities). Those entities are employed by automotive industrial and SME players to evaluate their products relying typically on certain standards or best practices. As long as the Common Criteria that constitutes the prominent approach or the SAFERtec framework is employed, the AFT can be used to significantly lower the involved costs and benefit all automotive stakeholders.

[2] A Common Criteria evaluation project (of a given product of average complexity) typically takes about 12 months to complete having a cost of up to USD $ 100K [3].

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

4 Conclusions

The AFT video demonstrator presents a brief yet representative view of the capabilities that the toolkit can offer. The document at-hand complements the video file offering further insights on the presented content.

The usage of the video demonstrator will be two-fold: on the one hand it will further assist the dissemination the SAFERtec achievements; on the other hand and more importantly, bringing this work in the attention of security evaluators (or even OEMs, automotive SMEs and Tier-1 providers) is expected to attract their interest and in line with the AFT acceptance, benefit the security evaluation of automotive products.

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

References

[1] The AFT code is publicly available at: https://isense-gitlab.iccs.gr/safertec/aft

[2] The SAFERtec modular Protection Profile: https://www.safertec-project.eu/publications/modular-pp/

[3] Lightship Security Common Criteria accredited laboratory e-book. Retrieved from https://lightshipsec.com/download/Lightship-7-Stepsto-Common-Criteria-eBook.pdf

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