Standardizing Security Evaluation Criteria for Connected Vehicles: A Modular Protection Profile

Konstantinos Maliatsos *, Christos Lyvas *, Panagiotis Pantazopoulos ‡, Costas Lambrinoudakis*,
Athanasios Kanatas*, Matthieu Gay¶ and Angelos Amditis‡
*University of Piraeus Research Centre, Piraeus, Greece
Grigoriou Lampraki 122, Piraeus 185 34
Email: {kmaliat, clyvas, clam, kanatas}@unipi.gr
‡Institute of Communication and Computer Systems (ICCS)
Email: {ppantaz, a.amditis}@iccs.gr
¶Airbus CyberSecurity, Elancourt, Ile-de-France, France
Email: matthieu.gay@airbus.com

***Abstract*—The so-far most credible approach to Security Evaluation, the Common Criteria standard, relies on a thorough methodology to provide confidence that the security requirements of an IT system are satisfied. Towards that end, a Protection Profile (PP) document gathers carefully all required data and identifies in an implementation-independent way the security requirements of the studied system, referred to as Target of Evaluation (ToE). When the *connected vehicles* paradigm that integrates a mosaic of third-party modules and interfaces constitutes the ToE, the PP development calls for agile solutions.**

In this work, we introduce a *modular* approach to the design of a PP for connected vehicles, as developed in the SAFERtec project. Our starting point is a generic architecture of the Vehicle (V-ITS-S) that helps us identify all involved assets and accordingly introduce a flexible discrimination of the base and associated PP modules as well as their interplay. We discuss the way our modular PP can cope with various V-ITS-S implementation approaches and provide insights on its applicability on a real-world V-ITS-S bench we have developed. The proposed solution can pave the way for devising standardized security assurance arguments towards safer connected driving.

I. Introduction

The emerging paradigm of *connected vehicles* [1], regardless its automation level, relies on the latest achievements of V2X communications, sensing capabilities and vehicle control algorithms to achieve safer driving conditions and improved comfort. Central to the corresponding cyber-physical system is the vehicle, referred to as *Vehicular-ITS-Station* (V-ITS-S) which embeds a multitude of hardware and software modules exposing a variety of interfaces (*i.e.*, wired/less and mobile). It therefore comes with an increased attack surface and a plethora of potential vulnerabilities [2]. Numerous sophisticated security controls have been introduced to mitigate identified threats [3], especially in view of safety concerns [4]. The question that subsequently arises is how to devise assurance arguments that will ensure that the V-ITS-S satisfies its intended (cyber-)security behavior.

Security assurance mainly amounts to the establishment of trust that a system fulfills its security requirements; the requested evidence is gained through carefully-designed evaluation processes for the complete development and operation cycle of the considered IT system, called the *Target Of Evaluation* (ToE). Clearly, the problem is challenging and is likely to remain so, given the ever-increasing complexity of IT systems and their rapid evolution. All existing IT security evaluation methods seek to cover three dimensions: a) What is to be evaluated; b) Which evaluation activities to follow and c) Which is the entity to perform the evaluation activities. However, each scheme has its own interpretation of what is important along these three dimensions and how to achieve it; thus, no 'universal' solution for security evaluation has been recognized, while criticism exists for all approaches [5].

Three are the most common security evaluation approaches: (i) conformity checks (ii) vulnerability tests (iii) and assurance frameworks. The first validates a system's compliance to a specific reference [6]. A reference conformity list relevant to the system's functional and security needs, has to be kept up to date. Typically, this is the fastest and cheapest evaluation scheme although anything not conformant to a subset of this list cannot be validated. Vulnerability tests [7] first require a quick perimeter definition *i.e.*, the product, the test environment and relevant limitations. Then, experts run tests of their choice seeking to reveal a set of security (potential) vulnerabilities. This method allows validation of the security compared to the state of the art, providing low to medium assurance level. The assurance framework approach [8] is the most complete achieving the highest assurance levels. Typically, it starts from a comprehensive description of the evaluation objectives and requirements and subsequently prescribes an exhaustive list of dedicated evaluation activities. Thus, it comes with considerable cost and time-to-complete calling for tailor-made enhancements to meet the connected vehicles' ecosystem needs [9].

The most widely recognized framework, is the Common Criteria (CC) for Information Technology Security Evaluation standardized in [10]. Starting from the security environment (*i.e.*, threats, assumptions *etc.*) and then understanding in-detail the system under analysis, CC describes the security objectives of the ToE. Drawing on them, the ToE security requirements can be prescribed in line with rationale state-

ments serving as evidence that the analysis is complete and internally-consistent. Towards that end, CC defines two important documents: The Protection Profile (PP) and the Security Target (ST). Both documents adopt a certain structure and terminology to formally define the involved security functional requirements (SFRs) and security assurance requirements (SARs). The difference is that PP describes requirements that are implementation-independent while ST describes requirements and mechanisms that are implementation-dependent and thus, of limited applicability.

This paper presents the position of the H2020 SAFERtec project [11] on how to assess in terms of security the use case of the connected vehicle. We propose an innovative way to apply the PP notion to the complex, heterogeneous and rapidly-changing automotive communication ecosystem; having adopted a generic V-ITS-S architecture that lends itself to a variety of real-world implementations, we have carefully designed and introduced a modular approach where the overall ToE and its corresponding PP breaks down into modules. The modular approach presents certain advantages: *Extensibility*: When considering another ToE such as the Road-side Unit, there is no need to study again the included communications units; the corresponding PP module of our solution can be used instead. *Upgradability*: New features or completely new modules can be attached to the PP without the need for a structural redefinition of the considered system. *Integration capability*: Existing and widely accepted PPs such as the one for the Hardware Security Module (HSM) [12] can be seamlessly integrated as modules.

Our proposal includes the base Protection Profile (base-PP), Protection Profile Module (PP-module) and Protection Profile Configuration (PP-Configuration) [13], defined for the V-ITS-S system in the context of the H2020 SAFERtec project [11]. The first one includes the V-ITS-S applications and related databases, addresses the basic functionality (to be installed in *all* types of V-ITS-S) and serves as a basis to build a PP configuration. Each of the PP-modules is an implementation-independent statement of security needs for the ToE and together with one base-PP compose the overall PP-Configuration which is used as a conventional PP for security evaluation.

The proposed PP not only intends to provide a methodology for security assessment of a heterogeneous system, but also proposes a set of (validation and penetration) tests as application notes of the security requirements. In addition, through testing and investigation of good practices, the PP will contribute in the recommendation of new ITS standards (*e.g.*, misbehaviour detection, position and time facilities, *etc.*) and the identification of vulnerabilities in existing ones.

The remainder of the paper is structured as follows: In Section II we present the so-far usage of PPs and subsequently in Section III we define the terms, assets and main modules involved in the introduced SAFERtec approach. Then, in Section IV, we provide guidelines on the applicability of our modular PP and in the following Section we detail an actual test-case of our PP on a real-world V-ITS-S bench we have developed. Section VI concludes the paper.

II. Related work

While PPs appearing in the CC portal [14] dates back to the late 90s, the idea of a modular PP is fairly new and so-far has not been applied on the automotive domain. To the best of our knowledge, the idea was firstly presented in the International Common Criteria Conference in 2013 [15]. A PP-module and PP-configuration were defined and a corresponding evaluation class was described to cope with the modularity characteristics. A Java Remote Method Invocation module and a Security Integrated Circuit were considered as application use-cases but none of them included the plethora of third-party components or raised the complexity of the connected vehicle ecosystem.

The following year ANSSI edited an addenda to the Common Criteria version 3 to extend the CC framework for the incorporation of modular protection profiles [16]. The document defines a methodology that allows addressing ToE's optional security features and enhances the factorization of PP evaluation tasks and PP maintenance processes by limiting the impact of any PP modifications.

The certMILS project [17] has been developing a modular protection profile for Separation Kernels. The Separation Kernel provides a basis for multiple partitions whereby the available resources (*e.g.*, the computer memory) are assigned to each partition. As such, the separation kernel constitutes an operating system with minimized functionality having more complex functions (*e.g.*, application management) being provided by individual partitions. In this case, their base-PP covers the basic functions of the Separation Kernel [18].

The considered ToE (*i.e.*, V-ITS-S as a whole) has been put under the microscope for a CC-based security evaluation for the first time. Compared to the above ToEs, it integrates numerous third-party components and exposes a variety of interfaces; we have therefore employed modularity-features to efficiently leverage the PP tool towards the (critical) automotive security assurance.

III. System Definitions

A. Target of Evaluation

The SAFERtec approach relies on the CC [14] and therefore adopts the CC system model, definition and terminology. In CC, the ToE is the cyber-physical system or product under evaluation. As SAFERtec ToE, the V-ITS-S *i.e.*, the high-level asset of the ITS ecosystem is defined. The V-ITS-S is defined as the complete set of assets, functions and functionalities that enable, support and essentially provide ITS services to the Connected Vehicle through network interfaces. In more detail, as V-ITS-S, we define all the hardware, software, networking and communication components installed on the vehicle, or any other device carried on it (*e.g.*, by passengers). SAFERtec aims at offering an end-to-end assessment approach, thus the ToE consists of many heterogeneous physical and logical modules that generate, handle, store or disseminate a plethora of information from numerous sources. The ToE objective is to provide ITS services through communication links between vehicles (V2V), links from vehicles to infrastructure (V2I,

e.g., road side units), as well as vehicle to an internet service (*i.e.*, the cloud-V2C) in a secure and reliable fashion.

B. The modular PP

In CC, one of the bases of the assurance procedure is the PP. The PP is a collection of threats, security objectives, assumptions, SFRs, SARs and rationales, defined and identified for a generic implementation-agnostic ToE. As part of the assurance procedure, the PP is a generic form of a CC ST, and it should be defined as a generalized implementation independent specification of information assurance security requirements. The PP is designed to characterize a given family of ToE implementations and it should define security functionality guidelines, as well as assist developers to fit specific products into a ST.

When designing the PP, a trade-off is formed:

- On the one hand, the ToE functionalities may be described with specific details imposing a strict functional architecture. In this case, the PP will be applicable only for those few systems that follow the specific architecture and it cannot be used for V-ITS-S that diverge from the architecture even by a single component.
- On the other hand, the ToE can be described more abstractly. With this method, the PP will be applicable on various architectures, designs and development scopes. However, due to its generic nature, it will not be able to provide strong security requirements since many functional details are omitted.

In SAFERtec, effort is made to build a PP that can be successfully applied in a variety of V-ITS-S implementations. This is a cumbersome task due to the complexity and heterogeneity of the V-ITS-S components. During the development of the V-ITS-S, hardware and software components from various OEMs and development teams are combined together to provide a large and highly complicated set of systems and services-from sensors and modems to applications and Human Machine Interfaces (HMI). The degrees of freedom in developing such a system are numerous, and it is impossible to propose a detailed architecture without fitting a specific implementation (and thus develop an ST rather than a PP).

The modular approach in the development of the PP is ideal for the structural and functional description of such cyber-physical systems like the V-ITS-S. The overall ToE and the corresponding PP breaks down to Modules making it easier to support multiple configurations and flexible architectures. Briefly, a Module is a PP of a specific high-level asset of the original ToE. For modules regulated and defined by standards and common best practices, the PP will embed an increased level of detail. Modules that are not as precisely defined and contain high level of abstraction, will be characterized by a more generic PP module with higher-level security requirement description. It is noted that the V-ITS-S PP is built based on the SAFERtec use cases, that correspond to Day 1 ITS services [1].

[1]In line with the "Day 1 applications" identified by the C-ITS platform.

The modular PP consists of the base-PP, the PP modules, and the PP configurations, but before defining these components, the high-level assets of the V-ITS-S should be defined.

1) V-ITS-S assets: In [19], the European Telecommunications Standards Institute (ETSI) has published a technical report summarizing the results of a Threat, Vulnerability and Risk Analysis (TVRA) for vehicle-to-everything (V2X) communications enabling ITS in 5.9GHz, *i.e.*, using the ITS-G5 radio standard. The TVRA was used as a guide and reference for this work. Thus, the definitions of the V-ITS-S system functional and data assets are based on those defined in [19]. The definition of the system assets is based on the high-level description of the functional V-ITS system components focusing on the functional objectives. The TVRA V-ITS-S assets are:

- *ITS Application(s)*, a set of functional assets that process ITS data for local use and determine when to initiate communications with other stations for ITS purposes.
- *Data Assets*, a set of databases relevant to the operation of the V-ITS-S, like the Local Dynamic Map (LDM), Local Vehicle Information (LVI) and Configuration/Profile data.
- *Protocol Control(s)*, the entity that selects/uses an appropriate message transfer processing procedure for an outgoing/incoming message. The approach used in the PP proposed in this work extends the role and functionality of the Protocol Control; a more appropriate term to describe the specific asset is *Communication Unit (CU)-Protocol Control*. The CU is defined as the physical or/and logical entity that implements and facilitates radio communication on behalf of the V-ITS-S.
- *Sensor Monitor*, consisting of the sensor, sensor firmware, driver and sensor log and configuration data. The most common sensor monitor asset met in V-ITS-S is the Global Navigation Satellite System (GNSS).
- *Vehicle System Control*, a set of functional assets to access the vehicle control systems allowing the ITS application to control vehicle behaviour. Nevertheless, for Day 1 applications, no actuators are considered, thus, the Vehicle System Control declines into the vehicle HMI for alarming/advising the driver.
- *Service Control* is probably the most challenging asset, since it is not bound with a specific hardware component or software module. It enables information exchange between vehicle assets. It manages the inter-process communication without altering the content of communications. Service control manages all the services and defines all access rules for the interaction between assets. In SAFERtec, the Service Control has an upgraded role since it also assumes the responsibility, for the management of the computational and storage resources and the respective interfaces and networks that are shared into the vehicle. In cloud computing terms, the basis of the Service Control is the V-ITS-S hypervisor and infrastructure manager, as well as all modules controlling the information flow between assets.

The next step on the design of the SAFERtec PP was to define the base-PP and the PP-modules. The identified high-level assets will be either considered as part of the base-PP or they will be "re-branded" as modules and they will be described by separate PP documents, *i.e.*, the PP-modules.

2) Base PP: The base-PP is the subset of system assets that are necessary for the implementation of any possible compatible V-ITS-S configuration. The base-PP should define a subsystem that can be investigated independently, and it simultaneously provides all interfaces and facilities for the interconnection of modules to the base in order to attach new functionalities, and capabilities to the overall system. The term V-ITS-S Base is used to describe the high-level V-ITS-S assets that are part of the base-PP.

The functionality supported by the V-ITS-S Base can be summarized by the following points:(a) it provides processing capabilities through the appropriate hardware and software components, (b) provides storage capabilities through the appropriate hardware components, (c) provides the required functionality for managing/controlling various communication interfaces that can be attached to the V-ITS-S Base, (d) implements the actual ITS application on the available resources.

Since the Base is the subset of system assets that are necessary for the implementation of any possible V-ITS-S configuration, the assets of the base-PP are: (a) the service control to implement inter-asset/inter-module communication and coordinate computing and storage resources, (b) the ITS application, (c) data assets, *i.e.*, databases like LDM and LVI that are necessary for the operation of the application and the system hypervisor.

3) PP-modules: A PP-module is an implementation independent statement of assets and security objectives for the given high-level ToE (*i.e.*, V-ITS-S) complementary to the base PP. Practically, a module is a high-level asset of the original ToE, that is not mandatory for the proper operation of the components of the base-PP. However, it offers a new set of functions and services accompanied with the corresponding security services when attached and used together with the Base. In a modular PP, the PP-modules address security features of a ToE that cannot be required uniformly for all products of this kind. This fits perfectly the complexity and implementation variety of the V-ITS-S.

Thus, each PP-module has a module-ToE, which is actually a high-level asset of the original ToE described in Sec. III-B1 not contained in the Base. Therefore, under the SAFERtec modular PP context, the PP modules are: (a) *the communication unit - protocol control*, (b) *the sensor monitor*, (c) *the vehicle system control - HMI*. The following notes can be made:

- In a given V-ITS-S, multiple instantiations of a module may exist. For example, an ITS may rely on multiple sensors and network interfaces.
- The CU is compulsory optional, meaning that at least one should exist. However, it is possible to have two or more and it is not considered mandatory to have, for example, both adhoc V2X and legacy cellular network connectivity. Generally, the fact that an asset may or may not be considered as part of the base-PP does not indicate lower importance in the ITS ecosystem, but it is a smart way to increase flexibility and versatility of the PP.
- In [19], the definition of the functional and data assets does not contain a cryptography module, which is considered in general a requirement for the V-ITS-S [12]. SAFERtec attempts to unify various approaches, like the risk analysis of [19] and the PP for the HSM produced by the Car2Car Communication Consortium. Thus, in SAFERtec, the HSM is also added in the list of modules and it is integrated in the modular V-ITS-S PP as a PP-module. In fact, the PP of [12] is used as a PP-module with minor differentiations.

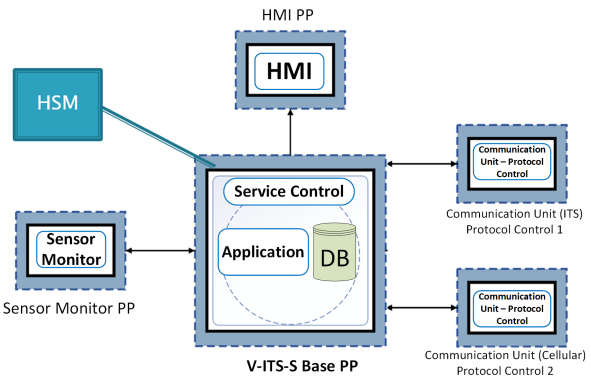

Fig. 1. The Modular Protection Profile architecture - a PP configuration

4) PP configuration: A PP-configuration results from the combination of at least one PP-module with the base-PP. The PP-configuration should in any case include the base-PP. In Fig. 1, a representative PP configuration is presented; the V-ITS-S is assumed to have two CU modules, *i.e.*, the system has two radio network interfaces, a V2X-ITS modem (*e.g.*, ITS-G5 or LTE-V2X) and a legacy 4G modem. It can also be seen that all modules can interconnect with each other through the base-PP and the service control asset. Thus, each module interfaces directly with the Base into a star layout. Finally, the HSM block is represented with different color, indicating that the specific module is described by an external PP [12], that is not developed by the SAFERtec project.

IV. Mapping of a real-world implementation to the SAFERtec PP

The first difficulty when trying to apply the SAFERtec approach on a real-world system is to fit the PP assets and modules into the hardware/software components that interact and cooperate with each other to realize the V-ITS-S system functionalities. This section aims to provide rules and guidelines in order to perform the mapping of the real-world components into assets and modules of the SAFERtec PP.

Generally, there are two basic implementation approaches regarding the hardware components used for the V-ITS-S:

- The centralized approach, where all (or the vast majority) of the system components is hosted by a single hardware

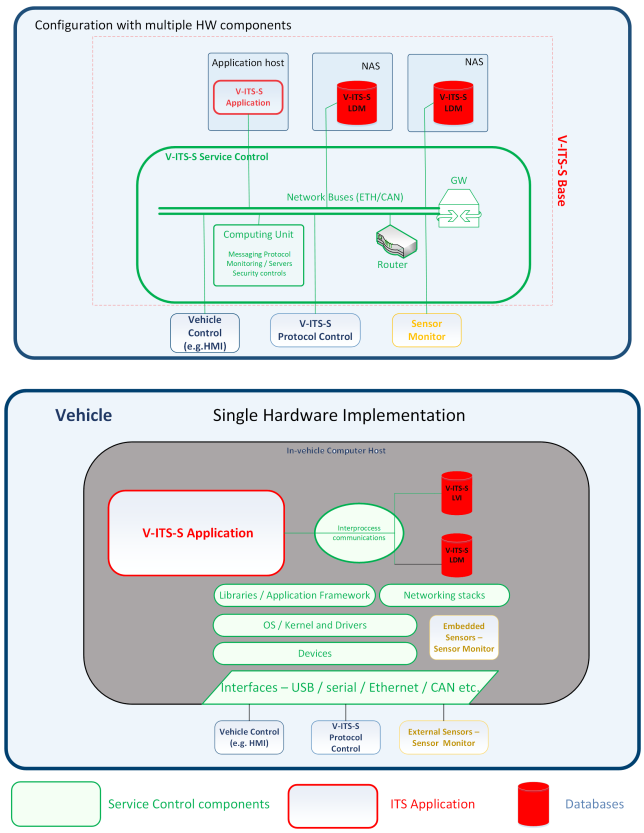

Fig. 2. (a) V-ITS-S as an integration of multiple interconnected components (b) V-ITS-S as a Single Hardware/Software unit

unit that can be considered as an in-vehicle super computer. All software is hosted into the specific hardware and all interfaces/connector are parts of the hardware peripherals.

- The distributed approach, where various pieces of hardware (usually coming from different OEMs) are interconnected with each other through interfaces and network components in order to compose the V-ITS-S

The two approaches are presented in Fig.2. In the centralized approach all assets are integrated into the same piece of hardware, where network interfaces and sensors are devices plugged on the system motherboard. On the other hand, in the distributed approach, each asset may be implemented by various hardware and software components and the interconnection of assets is facilitated by the in-vehicle network. Besides the purely centralized and distributed approach, a plethora of hybrid implementations can be considered, where some assets/modules are collocated into the same piece of hardware and others implemented as separate physical and/or logical components. It becomes clear that the system breakdown into the high-level assets may become a cumbersome task. In order to perform the distinction of components, the reader has to take into account the definition of each asset/module and based on the functionality of each hardware/software component, assign the component to an asset.

A. *Steps for asset/module distinction*

In order to facilitate the procedure of fitting the PP in a real-world implementation, the following rules are provided:

- All radio components (hardware) that implement the communication of the V-ITS-S with the external ITS ecosystem, are part of the Communication Unit asset.
- The firmware/middleware of the radio equipment is part of the Communication Unit asset.
- All software components implementing the Protocol Stack for the communication of the V-ITS-S with the external ITS ecosystem, from the Physical Layer to the Facility Layer is considered part of the Communication unit. The Application layer is excluded.
- All software components that manage and evaluate ITS information implementing the various ITS services and use cases are part of the Application asset. It is emphasized that the specific software components do not a) implement parts of the protocol stack (*i.e.*, part of the protocol control) or b) implement inter-asset communication of vehicle components (*i.e.*, part of the service control).
- Regarding the implementation of security functions like cryptography or integrity assurance algorithms, they are:
  - part of the protocol control if they are described explicitly by an ETSI ITS standard
  - part of the protocol control if they are implemented as part of the Physical, Medium Access, Radio Link, Network, or Transport Layer. In this context, they should be described by the mobile radio standard (e.g. LTE integrity, authentication and encryption protocols).
  - All other security services implemented in the Application Layer that are not explicitly described by the communication protocol standard are part of the Application asset.
- Key/certificate management and storage is performed by the HSM.
- All network components that implement the in-vehicle networking are considered part of the Service Control asset. All different interfaces (wired or wireless) are part of the Service Control, as long as they interconnect interior components of the V-ITS-S.
- All inter-asset communication is managed by the Service Control and thus it is considered part of the Service Control asset. Inter-asset communication in SAFERtec is assumed to follow a publisher-subscriber / producer-consumer/ request-reply scheme. All brokers and agents (software modules) implementing these functionalities are part of the Service Control. Software agents that play the role of the interface between assets and modules are also considered part of the service control.
- In-vehicle network routers and gateways are considered part of the Service Control.
- Shared storage space is considered part of the Service Control. External storage devices and interfaces for the attachment of storage devices (*e.g.*, card readers, USB interfaces, *etc.*) are part of the Service Control. Storage Space that remains internal to a specific asset (and it is not

shared externally in respect to the asset) is part of the specific asset. For example, a USB storage device on the CU, that is not accessible by any entity that is not part of the CU (internal or external to the V-ITS-S) is isolated and thus part of the Communication Unit.

- An Application Programming Interface, *i.e.*, a programming framework, libraries, functions, classes, *etc.* that allows and controls access to internal functional elements or data resources from entities beyond the boundaries of the application is considered part of the ITS application asset.
- Application Programming Interfaces exposed by other system assets, *e.g.*, the CU or the service unit used to disseminate relevant info (*e.g.*, signal strength, resources use, *etc.*) are considered part of the entity exposing the interface and should be considered a soft entry point inside the V-ITS-S.
- System databases that expose interfaces and data to assets, users and services inside the vehicle are part of the data asset of the system. Databases that remain interior to a specific asset, are not considered part of the data asset and they are considered local storage data of the specific asset.
- All computing units that are not embedded to sensors, the HMI or the CUs are administrated by the Service Control. The hardware component that hosts the Application and the LDM is part of the Service Control. The storage units hosted by the aforementioned computing units and possible Network- Attached Storage (NAS) are considered part of the Service Control.
- The HMI component includes:
  - a computing unit hosting the HMI application and services.
  - the software that implements the HMI.
  - the video display (usually touch-screen) and a video adapter that sends visual messages to the driver and/or the passengers.
  - audio adapter for audio notifications, warnings and alarms to the driver or the passengers.
- The HMI application should not be confused with the ITS application. The HMI is simply a presentation application
- The Sensor Monitor includes assets that provide relevant environmental data to the Service Control for distribution to the other functional assets of the V-ITS-S. Generally, Sensor Monitor module consists of the following components:
  - a sensor or else a source of information (through measurement) of an environmental quantity or a vehicle state.
  - the sensor firmware that provides low-level control for the sensor hardware. The sensor firmware is executed on processing units that control the sensor.
  - the sensor driver, *i.e.*, the computer process that operates and controls the sensor that is attached to a computing device. The driver plays the role of a software interface to sensor resources exposed on the Service Control. Sensor drivers are installed on Service Control hardware.
  - sensor local data, including log and configuration data. Sensor data may be stored locally on the sensor hardware or on storage units controlled by the Service Control.

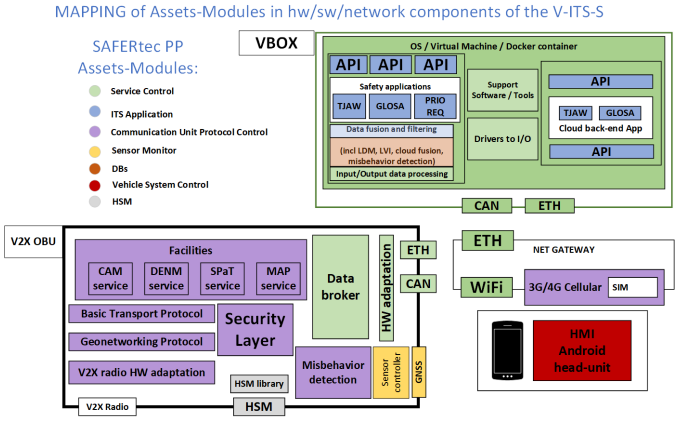

Fig. 3. Distribution of system components of the SAFERtec bench to high level assets of the SAFERtec architecture

V. A REAL-WORLD PP APPLICATION

As a test case, in order to test the effectiveness and applicability of the modular PP, a test-bench implementing all V-ITS-S system components was created. The SAFERtec test-bench is a challenging characteristic implementation that follows the distributed approach. Excluding micro-equipment and cabling, the SAFERtec implementation contains the following components:

- one ITS-G5 modem that interfaces with the other components through CAN or Ethernet. It is noted that the system HSM is collocated with the modem
- one Vehicle Computer (Vehicle box - VBOX) that provides all major computing and storage resources. The VBOX has CAN and Ethernet interfaces as well as conventional WiFi connection, that is considered out of scope for this work. The VBOX also hosts the ITS application, system data assets and several service control (hypervisor) entities.
- one LTE modem plugged directly on the VBOX.
- one HMI display (Android)
- a CAN bridge and an Ethernet switch.
- an indicative set of sensors. For the purpose of the test, a GPS is considered directly plugged on the VBOX.

The next step is to identify the functionalities provided by each sub-system. As an example, the ITS-G5 modem (denoted as On-Board Unit - V2X OBU) provides V2X radio connectivity and implementation of the protocol stack, as well as interfaces for the in-vehicle network. It also hosts the HSM (chipset and secure storage), as well as a messaging protocol broker for inter-asset communication and a GNSS device.

After having identified the functional entities for each device, the definitions, rules and guidelines of the previous sections were applied to the V-ITS-S implementation of the SAFERtec test bench in order to specify the context of each high-level asset/module of the V-ITS-S in line with the modular PP rationale. The result of the procedure is presented in Fig. 3.

In Fig. 3, physical, logical components or software entities are organized per device. Thus, it can be seen that the V2X radio stack is implemented on the modem device. However, the specific device also hosts logical or physical entities that are part of other assets/modules, like the HSM or the network interfaces and in-vehicle messaging protocols that are part of the Service Control. Regarding the VBOX, the Operating System or the virtual machine/container together with the (hardware/software) network interfaces and the messaging agents are part of the Service Control. On the other hand, the Applications providing ITS services hosted in the VBOX constitute the ITS Application assets. In the SAFERtec configuration, two ITS Application assets are considered: one using the adhoc V2X links and one using cloud services over the legacy cellular link. The Applications considered include Traffic Jam Ahead Warning (TJAW), Green Light Optimal Speed Advisory (GLOSA), and Priority Request (PRIO REQ)

Following the presented set of rules, the components of a V-ITS-S implementation can be classified in the proper high-level assets and modules of the modular PP. The methodology presented is implementation-agnostic and can be applied into any V-ITS-S architecture, regardless the host of each service or the number, type and nature of the application or network interface (radio and in-vehicle). A consequent major advantage of the SAFERtec approach is that new components or devices can also be added without the need for redefinition of the PP. If necessary, a new module will be defined and integrated into the PP configuration.

The next step in the security assurance procedure is to define the Security Target. This means that each module and its components is investigated separately as one logical subset. The respective PP-module is invoked and the satisfaction of objectives and requirements for the specific implementation of the module is assessed. As an example, the developed CU is assessed using the developed PP-module that includes description of 15 security objectives, 16 threats, 3 security functional policies and 9 organizational policies. The security assurance assessment is then performed by investigating the implementation of security controls based on 42 defined SFRs. The SAFERtec PP can be downloaded by the project website [11]. It is noted that they are subject to continuous revision and improvement taking into account suggestions, clarifications and feedback from stakeholders and relevant fora.

VI. Conclusions

In this paper, the SAFERtec modular PP for the V-ITS-S is presented. The development of a PP for such a complicated and heterogeneous system is a cumbersome task. The objective of this work is to use a modular approach in order to define a PP that can provide security assurance for V-ITS-S in a flexible, scalable and holistic way. The developed PP does not rely on a specific implementation architecture, nevertheless due to its modular approach it can assess in detail the security properties of the system. The generic architecture, the modules and configurations of the PP were described and a methodology on how the SAFERtec approach can be applied on real implementations was provided. Finally, the application of the modular PP on the SAFERtec test-bench V-ITS-S implementation is described. The application of the SAFERtec approach can provide security assurance and conformance with all relevant existed standards for a given product or service. The ultimate goal of the SAFERtec approach is to provide a reference for standardization of security evaluation for connected vehicles and ITS systems.

VII. Acknowledgments

This work is a part of the SAFERtec project. SAFERtec has received funding from the European Union's (EU) Horizon 2020 research & innovation programme under grant agreement No 732319. Content reflects only the authors' view and EU is not responsible for any use of the information it contains.

References

[1] N. Lu *et al.*, "Connected vehicles: Solutions and challenges," *IEEE Internet of Things Journal*, vol. 1, pp. 289–299, 2014.

[2] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, April 2015.

[3] M. Hashem Eiza and Q. Ni, "Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 45–51, June 2017.

[4] E. Schoitsch, C. Schmittner, Z. Ma, and T. Gruber, "The need for safety and cyber-security co-engineering and standardization for highly automated automotive vehicles," in *Advanced Microsystems for Automotive Applications 2015*. Springer Publishing, 2016, pp. 251–261.

[5] D. Mellado, E. Fernandez-Medina, and M. Piattini, "A comparison of the Common Criteria with proposals of information systems security requirements," in *First International Conference on Availability, Reliability and Security (ARES'06)*, April 2006.

[6] IEEE Conformity Assessment Program (ICAP). [Online]. Available: http://standards.ieee.org/about/icap/index.html

[7] H. H. Thompson, J. A. Whittaker, and F. E. Mottay, "Software security vulnerability testing in hostile environments," in *Proc. of the ACM Symposium on Applied Computing*, NY, USA, 2002, pp. 260–264.

[8] K. Beznosov and P. Kruchten, "Towards agile security assurance," in *Workshop on New Security Paradigms*, NY, USA, 2004, pp. 47–54.

[9] P. Pantazopoulos, S. Haddad, C. Lambrinoudakis, C. Kalloniatis, K. Maliatsos, A. G. Kanatas, A. Váradi, M. Gay, and A. Amditis, "Towards a Security Assurance Framework for Connected Vehicles," in *Fifth IEEE Workshop on Smart Vehicles: Connectivity Technologies and ITS Applications (IEEE SmartVehicles'18)*, Chania, Greece, Jun. 2018.

[10] "ISO/IEC 15408 part 1/2/3:2005-Information technology, Security techniques, Evaluation criteria for IT security," Tech. Rep., v3.1,Release 5. [Online]. Available: https://www.commoncriteriaportal.org/cc/

[11] The H2020 SAFERtec project website. [Online]. Available: https://www.safertec-project.eu/

[12] Car2Car Communication Consortium - V2XHardware Security Module PP. [Online]. Available: https://www.car-2-car.org/fileadmin/documents/Basic_System_Profile/Release_1.3.0/C2CCC_PP_2056_HSM.pdf

[13] The H2020 SAFERtec modular PP. [Online]. Available: https://www.safertec-project.eu/publications/modular-pp/

[14] Common Criteria portal. [Online]. Available: https://www.commoncriteriaportal.org/

[15] Modular Protection Profiles. [Online]. Available: https://www.yourcreativesolutions.nl/ICCC13/p/CCandNewTechniques/CarolinaLavatelli-ModularProtectionProfiles.pdf

[16] (Mar. 2014) CC and CEM addenda, version 1.0. [Online]. Available: https://www.commoncriteriaportal.org/files/ccfiles/CCDB-2014-03-001-CCaddenda-Modular_PP.pdf

[17] The H2020 certMILS project. [Online]. Available: https://certmils.eu/

[18] A. Ortega and S. Tverdyshev, "A compositional certification methodology for a COTS-based systems," *International Common Criteria Conference (ICCC)*, October 2018, Amsterdam, Netherlands.

[19] "Intelligent Transport Systems (ITS). Security, Threat, Vulnerability and Risk Analysis (TVRA)," Standard, Mar. 2017.