Multi-Layer Security Assurance of the 5G Automotive System Based on Multi-Criteria Decision Making

Jordi Mongay Batalla, Luis J. de la Cruz Llopis, Germán Peinado Gómez, Elżbieta Andrukiewicz, Piotr Krawiec, Constandinos X. Mavromoustakis, *Senior Member, IEEE*, and Houbing Herbert Song, *Fellow, IEEE*

***Abstract*— Security assurance is the capacity of any teleinformatic system to demonstrate that the system is secure. It is provided by testing the system by an independent laboratory. Such an evaluation gives to the customer certainty that the system or product is secure enough for the intended use. In this paper we discuss the security assurance that the automotive sector requires to the 5G network for the secure communication of the Intelligent Transport System applications. In this case, the automotive sector takes the role of the customer of the network operator that provides connectivity of cars, trucks, bicycles, pedestrians and traffic infrastructure for creating vehicle to everything platform. Concretely, in this paper we (1) show new methodologies for evaluating network security, (2) provide a new strategy for the customer (automotive company) to select the underlying system based on network assurance levels, (3) survey security functionalities of a network devoted to automotive applications and demonstrate how automotive applications, 5G network and physical infrastructure, cooperate for enhancing security of the end-to-end system, and (4) provide example security evaluation results at different assurance levels. The results show the necessity of providing different levels of network assurance during the certification process in order that the automotive customer will be able to select the best products and sub-systems that may demonstrate (assure) enough security to the complete system.**

***Index Terms*— Intelligent transport systems (ITS), communication system security, security assurance, security management, multi-layer security, multi-criteria decision making.**

Manuscript received 25 June 2022; revised 4 March 2023; accepted 9 October 2023. Date of publication 27 October 2023; date of current version 13 May 2024. This work was supported in part by the National Center for Research and Development in Poland under Grant 381282/II/NCBR/2018, in part by the National Science Foundation under Grant 2150213 and Grant 1956193, and in part by the Project titled "Smart and Health Ageing through People Engaging in Supporting Systems" (SHAPES) under Grant 857159. The work of Luis J. de la Cruz Llopis was supported by the Spanish Government under the Research Project "Enhancing Communication Protocols with Machine Learning While Protecting Sensitive Data (COMPROMISE)" funded by MCIN/AEI/10.13039/501100011033 under Grant PID2020-113795RB-C3X. The Associate Editor for this article was F. Qu. *(Corresponding author: Jordi Mongay Batalla.)*

Jordi Mongay Batalla and Germán Peinado Gómez are with the Institute of Telecommunications, Warsaw University of Technology, 00-661 Warszawa, Poland (e-mail: jordi.mongay.batalla@pw.edu.pl; german.peinado_gomez.dokt@pw.edu.pl).

Luis J. de la Cruz Llopis is with the Department of Network Engineering, Universitat Politècnica de Catalunya, 08034 Barcelona, Spain (e-mail: luis.delacruz@upc.edu).

Elżbieta Andrukiewicz is with the IT Security Evaluation Facility, National Institute of Telecommunications, 04-894 Warszawa, Poland (e-mail: e.Andrukiewicz@il-pib.pl).

Piotr Krawiec is with the IT Security Evaluation Facility, National Institute of Telecommunications, 04-894 Warszawa, Poland, and also with the Institute of Telecommunications, Warsaw University of Technology, 00-661 Warszawa, Poland (e-mail: p.krawiec@il-pib.pl; piotr.krawiec@pw.edu.pl).

Constandinos X. Mavromoustakis is with the Department of Computer Science, University of Nicosia, 2417 Nicosia, Cyprus (e-mail: mavromoustakis.c@unic.ac.cy).

Houbing Herbert Song is with the Department of Information Systems, University of Maryland, Baltimore County (UMBC), Baltimore, MD 21250 USA (e-mail: h.song@ieee.org; songh@umbc.edu).

Digital Object Identifier 10.1109/TITS.2023.3325908

I. Introduction

SECURITY is, in addition to performance, the main issue for the Automotive Industry to select the platform connecting the vehicles, the pedestrians and the infrastructure. The Industry needs proofs that the system will work secure with all its components, this is called Security Assurance. Security and Security Assurance are two terms related but not equivalent. Security is the capacity of a product to defend from attacks, whereas security assurance is the capacity of the product to demonstrate that the product is secure. Automotive companies will rely on the communications technology which demonstrates enough level of security.

The security is demonstrated during the evaluation of the products that form the system. An independent laboratory tests the products in regards to the implemented security. The tests go from simple security conformance tests (the product is conformant to the security standards) until complex penetration tests that aim to discover the potential security vulnerabilities of the product.

Current telecommunication products contain a number of sub-products or components, such as chipsets, communication modules, applets and many others. Each component may be evaluated separately and, then, the results of such an evaluation may be used for evaluating the composite product.

Each component of a product as well as each product of a system, may be evaluated for a different level of security assurance. This Evaluation Assurance Level (EAL) is related with the depth of the product tests that are specified based on the supplied product documentation. The tests span from security conformance tests or basic penetration tests that relay on simple vulnerability survey considering easily identifiable vulnerabilities (the lowest EAL), until complex penetration tests arising from advanced methodical vulnerability analysis

(the highest EAL). For example, Common Criteria (CC), an international standard for IT product certification [1], defines seven hierarchically ordered assurance levels, from EAL_1 to EAL_7, and each EAL_X includes all requirements and the tests envisaged for lower EALs.

All the products of the telecommunication system that are critical for the security (generally, all the network equipment) should be evaluated at a certain level, which should be related with the intended use of the system. For instance, in the automotive sector, manufacturers of ECUs (Electronic Control Units) must be compliant with the requirements of the ISO 21434 [38] and 24089 [39] standards. The producer of the equipment orders the evaluation of the equipment to the external laboratory. Then, the automotive companies, as the customer of the telecommunication system, will analyze the cybersecurity risks of the (automotive) sector and will decide the security requirements of the telecommunication supporting system. The requirements and cybersecurity risks will show the necessary security assurance level to be demonstrated by the supporting system. For example, an automotive company may decide that some key secrets are crucial for the functioning of the application and an attack to those secrets would have severe consequences, so then the system managing those secrets should demonstrate an assurance level 'High'.

This paper shows the implementation of an automotive network using 5G as the supporting telecommunication system and discusses the requirements of security assurance for the components of the system considering the Intelligent Transport System (ITS), the 5G Network Functions and the underlying physical infrastructure.

In Section II we explain the new approaches to security assurance evaluation that the market is requiring due to fragmentation and globalization of the supply chain. Globalization of the supply chain makes that telecommunication products contain sometimes dozens of components from different producers. Composed and multi-assurance evaluation are the responses to complex security assurance. We argue that multi-assurance evaluation offers higher flexibility for the selection of the products by the automotive companies.

In Section III, we present a novel strategy for the customer (automotive company) to select the underlying communication infrastructure by considering the security assurance levels of the products and sub-systems.

Section IV shows the security assessment of the Vehicle-To-Everything applications with the 5G as the communication platform. Security is assessed at the application (Vehicle-To-Everything, V2X), at the network and at the physical layers, and these layers may cooperate in the 5G environment in order to achieve higher security enforcement. We argue that 5G may fulfill the highest security requirements of the automotive sector.

Next, Section V presents real-time evaluation results of security functionalities shown by one example 5G Network Function which is crucial for automotive industry. The results show example penetration tests performed over a commercial implementation of the User Plane Function that require (the tests) increasing level of knowledge for compromising the evaluation target.

Based on the results of the tests and the discussion provided in previous sections, we conclude the requirements of the evaluation schemes dedicated to automotive sector in Section VI.

II. Multiple Component Security Assurance

Security assurance is the capacity of any component, product or system to demonstrate the level of the security defences. Security assurance is evaluated through a series of tests of the security functionalities (SF) of the so-called Target of Evaluation (TOE), i.e. the component, product or system. The security functionality (SF) is the designed defences of the TOE. The SF is described by a number of requirements (called Security Functionality Requirements, SFRs) of security posed to the TOE. These SFRs are the basis of the tests performed by an independent laboratory. The security functionality, and the resulting SFRs, derives from the product functionally and its intended use; however, one market sector (understood as a community of interest on one service) such as the automotive sector, may elaborate the security requirements of the products. The security requirements will be based on sector individual characteristics and specific context of use. In case of Common Criteria standard, such pre-defined set of security requirements are called Protection Profiles.

Currently, most of ICT (Information and Communications Technology) products contain several components from different producers. In this case, there are two main trends for conducting security evaluation: composite evaluation and multi-assurance evaluation. They depend on the description of the SF of the TOE.

Composite evaluation is an add-on for the security evaluation methodology defined in [1]. Composite evaluation has been developed and then implemented in smart cards [2]. Usually, a smart card consists of one of several components such as a chipset or chipsets, cryptographic processor, operating system located on the chips, libraries, module for communications and one or several applets. Different manufacturers can provide the different components; then, one can perform a security evaluation of the complex product by re-using its components' evaluations and adding only evaluations for interfaces among components themselves and between the product and the outside world.

Composite evaluations for smart cards are being performed primarily in European Common Criteria-based certification schemes, particularly in Germany, France and Netherlands. They are the most successful part of such certifications measured by the number of issued certificates [3].

Recently, the concept has been evolving by extending composite evaluations and considering different assurance needs of the components themselves, and it creates a basis for multi-assurance evaluations.

Multi-assurance evaluation is based on the fact that different assurance needs apply to different parts of the security functionality of the complex product. For instance, the producer assumes that some parts of a modular product require higher assurance than the rest. Before introducing multi-assurance, such needs would have forced a producer to undergo several evaluations of the same TOE for different specifications. With this concept, one can standardize and optimize this process

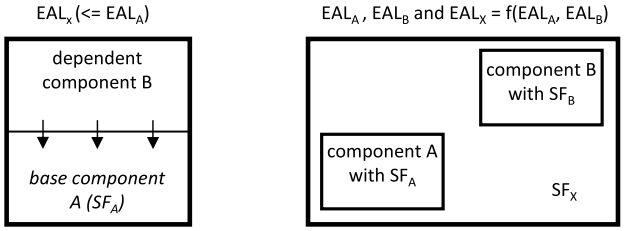

Fig. 1. Composite (left) and multi-assurance (right) evaluation.

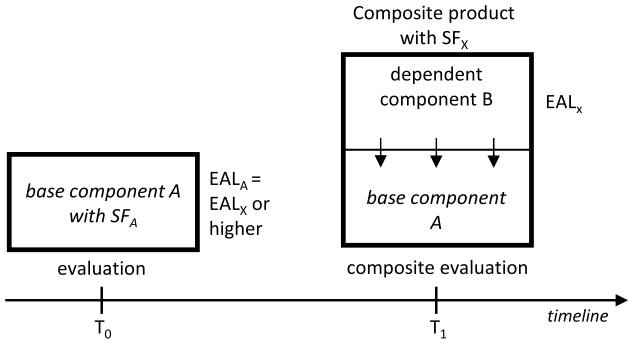

Fig. 2. Composite product evaluation process.

and determine the global assurance level for the product, which cannot be obtained by using the single-assurance approach [4].

It should be emphasized, that composite and multi-assurance approaches are focused on different requirements. Composite evaluation refers to products created as a stack (or chain) of dependent components, usually from multiple vendors, and it allows reusing results from previous evaluations. On the other hand, multi-assurance evaluation refers to a heterogeneous product that includes set of components with different security functionalities and requirements, in particular depending on the context and scenario of their application. The relationships between multi-assurance evaluation and composite evaluation are presented below.

A. Composite Evaluation

Let a product consists of two layered components, A and B, where the component B relies on services from the base component A (see Fig. 1-left). Typically, the producer of dependent component B makes use of base component A (provided by another producer). The producer of component B intends to order an evaluation of the composite product for a certain assurance level, say EAL_X. In the case of composite evaluation, separate security functionalities (SFs) for the components are not identified, only one SF for the composite product; the evaluation is based on this SF and the Security Functionality Requirements (SFRs) derived from it, and results in a targeted global evaluation assurance level EAL_X (which will be evaluated by the laboratory), see Fig. 1. Some SFRs may directly come from the security functionality of the base component A, while other SFRs will be related only with functionality of component B.

It is worth to remark that different SFs (specified by the vendor of the component) may provide to different EALs, so, for example, a base component that has SF_A related with a secure disk ciphering could obtain $EAL_A = EAL_5$, whereas the same component with an extended SF_A' defining two SFRs: secure disk ciphering jointly with secure communication at the interfaces, could obtain only the lower $EAL_A' = EAL_3$. This is an important characteristic of the SF, where each one of the SFR may obtain, if evaluated on the individual, a different level of EAL. At last, the EAL_X for the SF of composite product (containing all the SFRs) will not be higher than the assurance level demonstrated by each SFR. Therefore, in the case of composite evaluation, the definition of the SF of the components (and composite product) and the EAL, which the vendor aims to reach in certification process, need to go hand in hand. It is obvious that the client making use of the certified product will consider not only the SF of the product, but also the EAL of the certification process, and based on this, s(he) will be able to reject the product due to insufficient EAL.

A typical composite evaluation is performed in two steps: first, the base component A is evaluated at T_0, then the composite product that includes component A and dependent component B, is evaluated at T_1. The result is a targeted EAL_X for the composite product, as presented in Fig. 2. As explained above, there is a number of SFRs in the SF of the composite product that will address security functionalities of the base component A. The laboratory will make use of previous evaluation of the component A for those SFRs, however the laboratory may only do that if the EAL of the evaluated component A was, at least, EAL_X. Otherwise, the laboratory cannot exploit the results of the evaluation of the component A in order to reach EAL_X for composite product. Let us remark that the result of the evaluation process of the component A at T_0, is only the final assurance level demonstrated in tests (EAL_A), but there is no information about results of the tests regarding each SFR of the component A.

B. Multi-Assurance Evaluation

When a multi-assurance evaluation is considered, it is assumed that a product can be used in different scenarios, requiring different security assurance from specific components, for example, A and B as presented in Fig. 1-right. Therefore, components A and B are described by their security functionalities SF_A and SF_B, respectively, while SFX describes the entire product. In this way, it is possible to perform one evaluation with different specifications of security evaluation requirements for specific components and the entire product. This unique evaluation process results in specific evaluation assurance levels for the components (say EAL_A, EAL_B) and for a global evaluation level EAL_X for the entire product.

The global evaluation level EAL_X is related with EAL_A resulted from the evaluation of SF_A and EAL_B resulted from the evaluation of SF_B. However, the exact EAL_X in the multi-assurance approach is not precisely known. Please consider that there may be other SFRs for the product that are not related with components A and B. The specific role of the entity that integrates the entire system from the various components (it can be either a vehicle manufacturer itself or an external integrator) is to define which security functionalities

are needed for fulfilling the target security requirements. Next, the integrator must select from among the available components the functionality needed, while ensuring an adequate EAL.

C. Composite Multi-Assurance Evaluation

The multi-assurance approach can be applied to composite evaluation. The difference between composite and composite multi-assurance is that in composite evaluation, the final report of the evaluation done for the whole product (at T_1) does not contain any information about the previous evaluation of base component A (at T_0), whereas in composite multi-assurance evaluation, the final report of the evaluation of the whole product also contains information about the assurance level of the component A gained at previous evaluation (done at T_0). This way, the end user has information not only about the SF and EAL of the whole product, but also about the single component. An illustration of the importance of this information can be a home IoT gateway evaluated at a lower global EAL (say EAL_2) to keep the product price low. The gateway includes an xDSL communication module (base component) that is used to connect to the Internet, which was previously evaluated on EAL_4. Because the xDSL module exposes the gateway to the Internet, it is valuable for a user to be sure that special emphasis has been placed on the security of this component, appropriate to the potential threat. Moreover, the multi-assurance approach allows the EAL can be obtained also for other sub-modules of the product under evaluation, not only those covered by dependency relationship.

Thus, the composite multi-assurance security evaluation concept is more flexible than typical composite evaluation and can be further developed to answer the needs for sectorial market (such as automotive) that requires a secure communication network. The strategy of the automotive companies for selecting the supporting communication system is presented in the next section.

III. Security Assurance of Supporting Communication Systems for ITS Purposes

When an ITS customer (e.g., cars or trucks manufacturer) aims to select or develop a telecommunication system with security requirements, she/he will install certified products that demonstrated enough level of security assurance for the intended use. It is responsibility of the customer (or the sector, which the customer belongs to) to do a risk assessment plan for the intended use of the system. From that plan, the security requirements for the system and the required level of security assurance will be derived. Such pre-defined set of security requirements and desired EAL are focused on the characteristics and needs of the sector concerned [42], and imposes on manufacturers which security functionalities their products should offer and what evaluation they should undergo.

In a complex IT system such as a network providing nationwide connectivity for ITS, several sub-systems interwork in the complete security framework. As we will see in the next section, for ITS systems, at least: ITS security, network security and physical infrastructure security, need to be considered, each one containing many different products that may demonstrate different levels of security assurance.

We assume that there are several suppliers for each subsystem, so that the overall network may be constructed from sub-systems provided by different vendors. As an example, we may think about a sub-system that holds the security keys of the network subscribers. Such a system will have high security requirements including physical access security to the servers.

The sub-systems will normally be composed by several products, and these by several components. In composite evaluation, any of the components has not defined security functionalities, so the customer may only consider the SF of the whole product. Any product fulfilling the requirements from the customer and accomplishing $EAL_X \geq EAL_Y$ will be acceptable for the development of the system.

In multi-assurance evaluation, each component has its own SF and, as a result of the evaluation, its own EAL_n, n=1.. N, where N is the number of components in the product with specified SF, whereas EAL_X is the Evaluation Assurance Level of the whole product. In this case, the customer will consider which components operate the needed security requirements and the security assurance level that the components may demonstrate, and will select the products with components that show necessary security assurance at a certain level.

We propose a strategy for the ITS customer to select the communication system that will support the ITS system. This strategy is based on several criteria that need to be considered, some of them are inclusive/exclusive such as the EAL of the products (a product has enough security assurance or it does not have).

Let $p = \{1,.., P\}$ be the components or, in general, products of a sub-system, each product p having (1) separate security functionalities SF described by a set of security functionality requirements, and (2) separate evaluation assurance level EAL_p.

The alternatives are the sub-system implementations from different vendors (e.g., different solutions of public cloud at the physical infrastructure or different deployments of User Plane modules at the network layer), each sub-system containing several products and, thus, represented by an element in $EAL = EAL_1 \times EAL_2 \times \ldots \times EAL_P$.

As explained above, evaluation at higher level will include all the evaluation tests done at lower level, so we may introduce a preference relation $\prec$, $\succ$, $\precsim$, $\succsim$, over the sub-systems. Obviously, the selection of the telecommunication system will be based not only on evaluation level but also on other parameters such as price, business interests and policies, and others [5]. Thus, for completeness purpose, the representation of each alternative will be generalized to n attributes $A = A_1 \times A_2 \times \ldots A_N$, where P first attributes will refer to the EAL values of the P products or components and (N-P) attributes will refer to other business parameters.

In this case, the preference relation is represented by an utility function $Util : A^N \rightarrow \mathbb{R}$, such that alternative $alt1 alt2$ if and only if $Util(alt1) \geq Util(alt2)$.

Let us assume so-called weak separability of the N attributes. The weak separability means that the preferences over one attribute should be independent of the other attributes, i.e., $alt1 = A_1^1 \times A_2^1 \times \ldots A_N^1 \succsim alt2 = A_1^2 \times A_2^2 \times \ldots A_N^2 \leftrightarrow alt1 = A_1^1 \times A_2^{1*} \times \ldots A_N^{1*} \succsim alt2 = A_1^2 \times A_2^{2*} \times \ldots A_N^{2*}$.

In the network sub-system's selection presented above, the weak separability is a straightforward consequence of the assumed decision process since one alternative may be preferred to another by any of the value of EAL (or any business policy) in an independent (not conditioned to other attributes) way. This feature allows to order the selection preference, such that $\forall alt1, alt2 \in A, where\ A_n^{alt1} \geq A_n^{alt2}, n = \{1, .., N\} \rightarrow Util(alt1) \geq Util(alt2)$.

Preference relation with weak separability allows to define the utility function of one attribute, also called value function, as $u(A_i) : A_i \rightarrow \mathbb{R}$, and the utility of the alternative as a function f of the utility of each attribute $u(A_i)$:

$$f : \mathbb{R}^N \rightarrow \mathbb{R}, such\ that\ Util\,(alt1) = f\left(u\left(A_1^1\right), u\left(A_2^1\right), .., u\left(A_N^1\right)\right) \quad (1)$$

Weak separability obliges $u(A_i)$ to be a non-decreasing function since, as we defined previously, the utility function is consistent with $\prec, \succ, \precsim, \succsim$ preference, so $u\left(A_j^1\right) \geq u\left(A_j^2\right) \leftrightarrow A_j^1 A_j^2$.

By assuming weak separability, we may consider the attributes $j = \{1,.. P\}$ separately from the attributes $i = \{P + 1,.. N\}$, such that we may estimate the utility function for EAL attributes and for business policies separately.

There are several strategies for the utility function $f : \mathbb{R}^N \rightarrow \mathbb{R}$. We propose to use the well-known model of capacity [6]. This model proposes some levels of the attributes for which the attribute is considered unacceptable, acceptable, advisable, optimum or any other qualifier that make the attributes comparable. The comparability of the attributes is a key issue for making decisions in multi-criteria problems since the space of attributes is not generally a normed space. If the space of attributes would be a normed space (i.e., there is a norm $A^N \rightarrow R$ with the properties of distance: (1) the norm is ≥ 0; (2) the norm is $= 0$ iff $A^N = 0$, (3) it has the triangle inequality and (4) it is multipliable by a scalar), then the utility function could be a distance function (e.g., Minkowski distance).

In our case, the business policies and evaluation levels are not a normed space (there is not a norm that connects them). Therefore, we assume that it is possible to qualify the attributes. This is done by the reference levels of the capacity model.

In capacity model, we define L_i levels for the values of $A_i, i = \{1, .., N\}$. The L_i reference levels will define $\{L_i+1\}$ intervals of attribute A_i as follows: $\left[0, Q_1^-\right[, \left[Q_1, Q_2^-\right[, .., \left[Q_{L_i}, \infty\right[$, such that $A_i^{alt} \in \left[0, Q_1^-\right[\cup \left[Q_1, Q_2^-\right[\cup .. \cup \left[Q_{L_i}, \infty\right[$.

For each one of the $\{L_i+1\}$ intervals we define the utility function $u(A_i) : A_i \rightarrow \mathbb{R}$ as a constant value C_j in the interval $\left[Q_j, Q_{j+1}^-\right[$. As the function $u(A_i)$ must be nondecreasing, then: $C_i \leq C_j \leftrightarrow \forall p \in \left[Q_i, Q_{i+1}^-\right[, \forall q \in \left[Q_j, Q_{j+1}^-\right[\rightarrow p \leq q$.

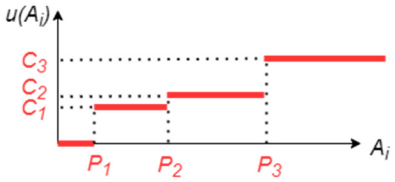

Fig. 3. Example of utility function $u(Ai)$, $i = \{1,.., N\}$, for $L_i = 3$.

The formal definition of $u(A_i) : A_i \rightarrow R$ is:

$$u\,(A_i) = \begin{cases} 0 & iff\ 0 \leq A_i < Q_1 \\ C_j & iff\ Q_j \leq A_i < Q_{j+1} \\ C_{L_i} & iff\ Q_{L_i} \leq A_i \end{cases}$$

So-defined $u(A_i)$ is non-normalized. The normalization process is immediate by dividing all the constants C_j, j={1,..,L_i} by value C_{L_i}, such that $u\,(A_i) \in [0, 1]$.

$$u\,(A_i) = \begin{cases} 0 & iff\ 0 \leq A_i < Q_1 \\ C_j/C_{L_i} & iff\ Q_j \leq A_i < Q_{j+1} \\ 1 & iff\ Q_{L_i} \leq A_i \end{cases} \quad (2)$$

Fig. 3 shows an example of utility function $u(A_i)$.

There are many other potential utility functions that accomplish the nondecreasing condition, however the threshold function well approximates the human reasoning (we often classify situations by using the threshold function) and the business policies are the result of human reasoning.

It is worth to remark that in business policies the number of reference levels will be not high. For example, three reference levels could be for four intervals: "unacceptable", "tolerant", "advisable" and "optimal".

In the case of EAL attributes, the intervals are only unacceptable and acceptable, as it has been discussed in the previous section. If we assume a given level of network security EAL_X for the whole sub-system, the decision strategy will oblige all the EAL attributes to be $EAL \geq EAL_x$ and any $EAL > EAL_x$ will not provide any added value to that attribute. Therefore, in order to estimate the utility function *$u(A_i)$ for EAL attributes* (i.e., *i={1,..,P}*), we use the feature of weak separability and define the function $u(A_j) : A_j \rightarrow \mathbb{R}$ of the EAL attributes, i.e., $j = \{1, .., P\}$ as a one reference level function, as defined in (3).

$$u\left(A_j\right) = \begin{cases} 0 & iff\ A_j < EAL_X \\ 1 & iff\ A_j \geq EAL_X \end{cases} \quad (3)$$

If any of the EAL attributes of the alternative alt is lower than EAL_X, then the alternative *alt* should not be selected since at least one product has not demonstrated enough security assurance. This means that formula (1) is defined as in (4):

$$f\,(u\,(A_1), u\,(A_2), .., u\,(A_N)) = \prod_{j=1}^{P} u(A_j) \times g\,(u\,(A_{P+1}), .., u\,(A_N)), \quad (4)$$

where $g : \mathbb{R}^{N-P} \rightarrow \mathbb{R}$ is the utility function for the non-EAL attributes (i.e., other business policies).

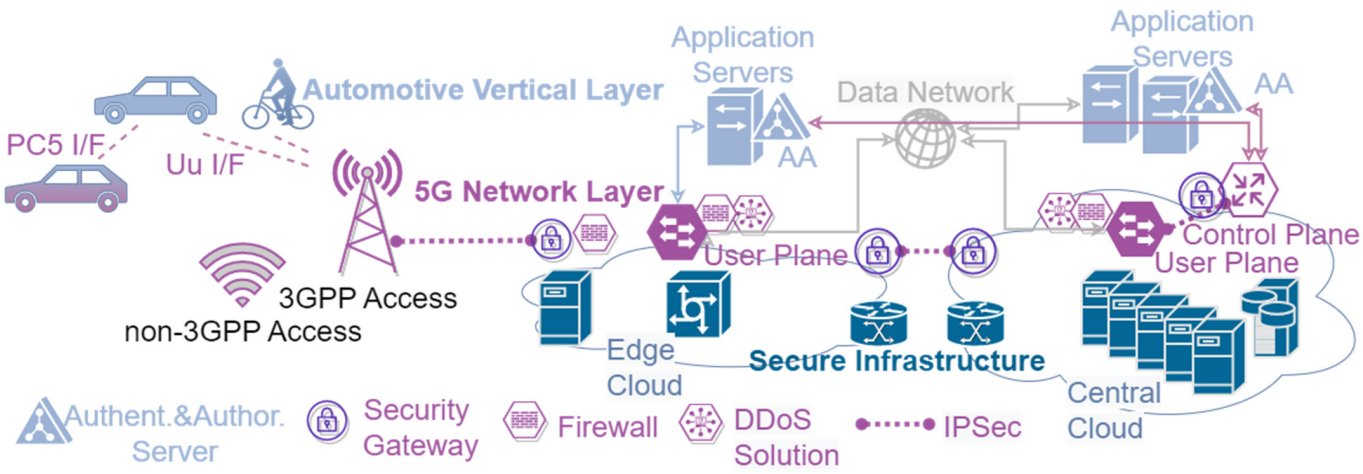

Fig. 4. Three-layer security assessment for automotive industry: Automotive vertical layer, 5G Network layer and secure infrastructure.

In formula (4) any value $u(A_i) = 0, i = \{1, .., P\}$ will make $f(u(A_1), u(A_2), .., u(A_N)) = 0$, which means that if a sub-system contains a product with $EAL<EAL_X$, such a sub-system cannot be selected (its utility is 0).

For the other business policies ($u(A_i)$, $i+\{P+1,.., N\}$), we should observe that the function $g : \mathbb{R}^{N-P} \rightarrow \mathbb{R}$ is further weakly separable, otherwise f would not be weakly separable for all the attributes. This is not acceptable in our model, as discussed above.

The intervals defined as quality features of the attributes (unacceptable, tolerant, etc.) provide the intuition that alternatives that have one or more attributes of business policies in lower intervals should be discarded (even if all the other attributes are in high-level intervals) in comparison to other solutions that have all the attributes in medium-level intervals. This is a heuristic strategy achieved by the minimax function.

For applying the minimax function the attributes need to be normalized and, in the case that we use quality features to describe the intervals, then they should be equal for all the attributes, i.e., $L_i = L_k \forall i = \{P+1, ..N\}, \forall k = \{P+1, .., N\} \cap C_j^{attr.i} = C_j^{attr.k} \forall j = \{1, .., L_i\}, \forall i = \{P+1, ..N\}, \forall k = \{P+1, .., N\}$.

In addition, in our case the minimax function should be applied to the whole function $f(u(A_1), u(A_2), .., u(A_N))$, see formula (4).

Therefore, we first need to define the function $g : \mathbb{R}^{N-P} \rightarrow \mathbb{R}$ as the minimum function:

$$g(u(A_{P+1}), .., u(A_N)) = \min_i u(A_i), i = \{P+1, .., N\},$$

where $u(A_i)$ is as defined in (2).

Then, the final function $f : \mathbb{R}^N \rightarrow \mathbb{R}$ of the utility of each attribute is defined in (5).

$$f(u(A_1), u(A_2), .., u(A_N)) = \max_{alternative} \left(\prod_{j=1}^{P} u(A_j) \times \min_{i=\{P+1,..,N\}} u(A_i) \right) \quad (5)$$

where $u(A_j)$ is defined in (3), and $u(A_i)$ is defined in (2).

IV. Multi-Layer Security Assessment for Automotive Connected Through 5G Network

In this section, we present the sub-systems that integrate automotive systems with the 5G network and we show how the sub-systems may collaborate to obtain enhanced end-to-end security.

From the point of view of security, autonomous cars/trucks connected to everything (other cars, pedestrians, traffic control infrastructure, etc.) rely on a secure communication at the application level (automotive vertical layer) as well as on a secure and reliable underlaying network [7]. 5G has been designed with the thinking of supporting such applications.

Security is then constructed and demonstrated, at least but not at most, over three different layers. At layer of autonomous cars/trucks, the data must remain confidential and their integrity must be protected. At the same time, the network must demonstrate to be secure in order that any communication with the exterior will prove solid and reliable. At last, the network (that from the 5G is softwarized) relies on physical equipment that, on its turn, must demonstrate security reinforcement to avoid attacks to the physical layer. Fig. 4 shows security deployment in three-layer infrastructure. The next sub-sections present details of the security exaction in the layers and the interfaces between the layers for security functionalities.

All the following security functionalities should be evaluated at a certain level related with the intended use. In the case of ITS, the risks are high and, thus, the security assurance level should be proportional to those risks.

A. Security at the Automotive Vertical Layer

In the communications architecture proposed by the European Telecommunications Standards Institute (ETSI) for Intelligent Transport Systems (ITS) [8], the ITS stations (ITS-S) collaborate to provide traffic management and safety services. These ITS-S are mainly grouped into four groups: vehicles (On-Board Equipment, OBE), infrastructure

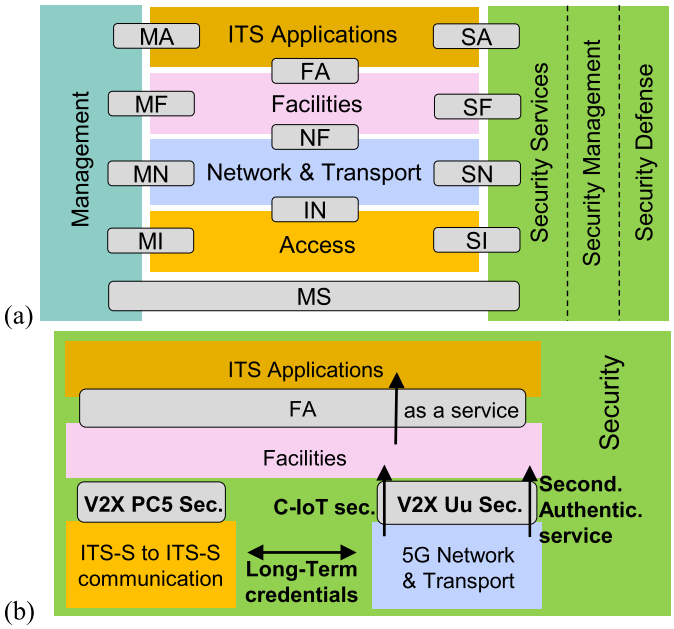

Fig. 5. (a) ETSI ITS-S reference architecture. The letters of an interface between two layers is called by the first letter of each one of the layers; (b) architecture adapted to 5G usage with description of Security interfaces.

(Road Side Equipment, RSE), personal (mobile phones, PDAs, etc.) and centrals.

The ITS-S reference architecture is shown in Fig. 5(a), whereas the adaptation of the reference architecture to the case of 5G connectivity is presented in Fig. 5(b). In the latter, the 5G introduces mechanisms for increasing security for trusted vendors applications. This is the reason of the vertical interfaces in Fig. 5(b). Moreover, the 5G does not separate the access and the network since the applications may be run directly at the edge (e.g., Multi-Access Edge Computing, MEC), i.e., in the access network. However, 5G makes direct communication between ITS-Stations (ITS-S) feasible, as shown in Fig. 5(b). Detailed explanation of the security interfaces and mechanisms may be found in the next section.

In the reference architecture, see Fig. 5(a), the two topmost layers are typical of the automotive applications. Different classes of applications can be considered, with more or less stringent requirements in terms of reliability, latency and security. The Facilities Layer defines some services and protocols to give support to the applications, such as the Cooperative Awareness Basic Service and the Cooperative Awareness Messages (CAM) to exchange ITS-S status, position and speed [9], or the Decentralized Environmental Notification Basic Service and the Decentralized Environmental Notification Messages (DENM) to alert road users of a detected event [10]. In the Networking & Transport Layer, two main possibilities are taken into account: the classical TCP/IP protocol stack, and the Basic Transport Protocol (BTP) together with the Geonetworking approach. At the Access Layer, several technologies are considered, including among others IEEE 802.11p/bd and 4G/5G networks for C-V2X. These two technologies are currently the most widely considered to support ITS. On the one hand, IEEE 802.11p technology appeared in 2010 as an annex to the IEEE 802.11 standard for wireless local area networks (WLANs), oriented to wireless access in vehicular environments, and was definitively incorporated into the global standard since the 2012 revision [35]. This technology is taken as the basis for dedicated short-range communications (DSRC), and in the ETSI environment it is standardized as ITS-G5 [36]. A new improvement, IEEE802.11bd, has been recently released [37], for V2X communications in 5.9 GHz and 60 GHz frequency bands. On the other hand, C-V2X technology for cellular networks is currently based on the 5G-NR standard. Both 802.11 and C-V2X have advantages and disadvantages, being currently an open topic of discussion which is the most suitable for each application environment. Looking at overall security issues, cellular networks present an infrastructure that can be considered more robust and is the solution towards which OEMs are tending, which is why it is the option considered in this work.

With respect to the management entity, ETSI-ITS contains management elements that may be grouped into four main groups: application, station, cross-layer and regulatory management [11].

The security management services and roles, as well as the security architecture, are defined and detailed in [12] and [13]. Even though in Fig. 5(a) the Security Entity is shown as a vertical layer adjacent to each of the ITS layers, the same standard [8] points out that security services are provided on a layer-by-layer basis. The same occurs to Management.

Therefore, in Fig. 5(b) we present details about how security is managed in the layers and the security functionalities spanning through different layers.

At ITS application level, the system must provide security processing services (Security Associations management, sending and receiving secured messages, etc.), security management (enrolment in the ITS domain, authorization tickets management, etc.) and security defence (plausibility validation, misbehaviour detection, etc.).

ITS applications can be classified into four main groups: active road safety, cooperative traffic efficiency, cooperative local services and global internet services. Depending on the nature and group to which each application belongs, the security needs will be different [13]. For example, for the cooperative awareness service (CAM messages), authenticity and integrity are required, as well as the authorization to send messages. For authentication and authorization, different levels may apply. 5G provides a service for Third Parties to authenticate their clients by using the network authentication based on keys stored in customer's SIM/eSIM card. With this service, ITS will be able to authenticate ITS-S by contacting the 5G network and using credentials of the network authentication. This is pointed out in Fig. 5(b) with the authentication service offered by the network layer to the application layer, and will be discussed below in this text. Besides, as these CAM messages contains information belonging to the sending station, privacy must also be assured. Finally, as the rest of the stations must be able to interpret the carried information, confidentiality is not necessary. On the other hand, for a static local hazard warnings service, the source of the DENM messages is the Road Side Unit, and therefore the authenticity,

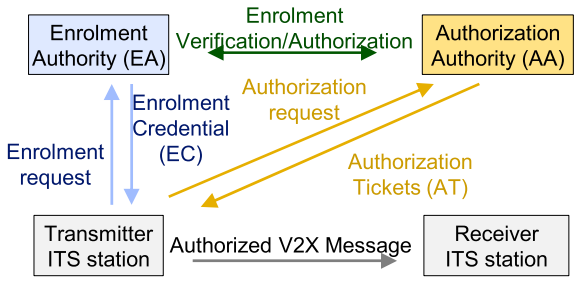

Fig. 6. ITS-S enrolment and authorization processes.

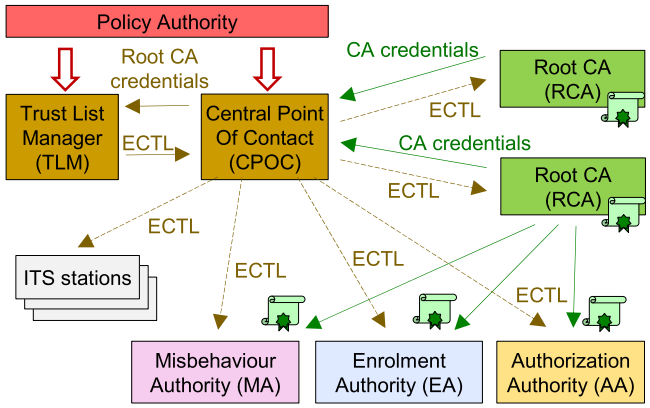

Fig. 7. Functional elements for trust management with multiple Root CAs. CTL- Certificate Trust List.

integrity, authorization and confidentiality needs would be similar to the previous case, but the privacy would not be necessary.

The architecture of the Cooperative-ITS Security Certificate Management System (C-ITS Trust Model) includes the Enrolment Authority (EA), the Authentication Authority (AA) and the Root Certification Authority (Root CA). The Security Lifecycle for an ITS station begins with an initial setup during manufacturing [14]. In this step, a canonical identifier, which is globally unique, is assigned to the ITS-S. Besides, the network addresses and public key certificates of the EA and the AA are also provided to the station. In the second step, to enrol in the ITS domain, the station sends its identifier to the EA, which checks its validity and provides the enrolment credentials (EC), as it is shown in Fig. 6. With these credentials, the ITS-S is able to request Authorization Tickets (AT) to the AA, which allows to send secured messages, such as CAMs or DENMs, to other stations.

Apart from the EA and AA, the station can also communicate with a Misbehavior Authority (MA), to report possible sabotage attempts detected from other stations. At the highest level of the hierarchy there is the Root CA, who certifies the validity of the EA and the AA to provide ECs and ATs, respectively.

In the case of multiple Root CAs involved in the C-ITS, the architecture shown in Fig. 7 is used. The different Root CAs provide their certificates to the Trust List Manager (TLM), optionally (in practice it is commonly used) through a Central Point of Contact (CPOC). The TLM is authorized by the Policy authority (composed by public and private stakeholders), who also decides if the Root CAs are trustable. With this information, the TLM creates and signs the Root CA certificate list, in the form of Certificate Trust List (CTL) and makes it available to all interested entities.

B. Security at the Network Layer

3GPP Working Group SA3 specifies the security requirements, features and procedures for the 5G system in [15]. As standardization aims at ensuring interoperability, the 3GPP security normative specifications focus on securing the 3GPP-specified interfaces [16].

Diligent design and implementation of general network security mechanisms such as perimeter security, network zoning, traffic separation or firewalling among others, are required building blocks in every mobile network. Additionally, new schemas such as Zero Trust Architecture (ZTA) [17] will impact the security assessment of the 5G.

To build a security framework in 5G networks the following main areas are to be considered in the design, independently of the services and applications to run on those networks:

- Standard security architecture (3GPP);
- Non-formally standardized security best practices and schemas;
- Security Operations;
- Security assurance of the network elements and the systems building the architecture.

In addition, there are specific security areas for third party applications such as ITS systems, which will be shown in the next sub-section.

Services and applications, enabled by 5G networks require an end-to-end Service Orchestration layer as defined in [18] when network slicing is deployed. Security orchestration shall be an integral part of that layer, ensuring the security levels across the entire network and providing automation in the enforcement of the security policies and controls (e.g., strong authentication, security audit logs, roles and/or attributes-based access controls, etc.). Network Slicing in particular requires secure procedures to create and instantiate network functions and security functions on demand, as well as to maintain agreed security service level agreements with tenants. These aspects are typically managed in Security Operation Centres (SOCs), together with the usual processes of security monitoring, event and incident management.

With the exception of some radio network elements with air interfaces, most of the Network Functions (NFs) building the 5G network are deployed in a virtualized, cloud-based infrastructure. Multiple deployment variants are indeed possible in private, hybrid or even public clouds, which host in central and/or distributed data centres (e.g., Mobile Edge Computing) the functions and applications of the 5G system. Therefore, cloud security mechanisms play a key role in the overall 5G security framework.

Fig. 8 provides a schematic high-level view of the 5G architecture, where the main security elements and features have been highlighted. Please note that the notation of the schema does not include the names of the network functions

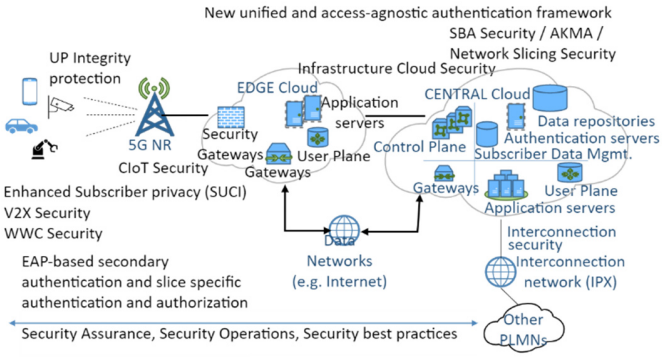

Fig. 8. 5G Security building blocks.

specified for the 5G system, but for simplicity only key functionalities have been mentioned.

Since the conception of 5G, security has not been regarded as an add-on only; instead, security has been considered as part of the overall architecture and built into the architecture right from the start [16].

5G security architecture has been specified in [15] and built across six security domains, i.e., network access security, network domain security, user domain security, application domain security, SBA domain security and visibility and configurability of security. Those domains are relevant to position the security features within the architecture. The foundation features were the following:

1) New Unified and Access-Agnostic Authentication Framework: The 5G system supports two main authentication methods: 5G-AKA (Authentication and Key Agreement) and EAP-AKA' (Extensible Authentication Protocol for AKA). Both mechanisms can be applied for 3GPP as well as for non-3GPP access, and both provide assurance to the home network that the User Equipment (UE) is present in the visited network, what brings a significant improvement in home Public Land Mobile Network (PLMN) control in roaming scenarios. Besides EAP-AKA' other EAP methods such as EAP-TLS can be implemented for example in non-public networks and vertical industries (e.g., in the authentication of Wi-fi devices). The support of EAP-TLS within the 5G system is a further step to facilitate the integration with verticals and enterprises [19].

2) Enhanced Subscriber Privacy: 5G enhances the privacy posture in previous mobile network generations preventing that the SUPI (Subscription Permanent Identifier) was never sent in the clear over the air interface. In a public network SUPI contains an IMSI (International Mobile Subscriber Identity). There is a specific schema to encrypt a SUPI in case it has to be transmitted from the UE to the network building a new identifier known as SUCI (Subscription Concealed Identifier). The UE computes the SUCI by encrypting (Elliptic Curve Integrated Encryption Scheme, ECIES) the individual part of the SUPI (MSIN: Mobile Subscriber Identification Number) with a public key pre-provisioned in the UE. The network decrypts the SUCI using the Subscription Identity De-concealing Function (SDIF). Note that mostly the 5G-GUTI (Globally Unique Temporary Identifier) is used over the air, and there are stringent requirements for frequent allocation of a new GUTI.

3) User Plane (UP) Integrity Protection in Radio Access Network: UP integrity includes both confidentiality (encryption) and integrity protection and is mandatory to support and optional to use. This means that the use of IP integrity protection will be negotiated between the UE and the network. The negotiation is done per PDU (Protocol Data Unit) session and the Session Management Function (SMF) is in charge of sending the policy decision down to the gNB (5G base station), where the policy gets applied Radio Bearer-specific basis.

4) Service Based Architecture (SBA) Security: Two basic security mechanisms have been standardized to protect the service-based interfaces of SBA (both mandatory to support, and optional to use):

- TLS with client and server certificates (a.k.a. mutual TLS) between all network functions;
- Token-based authorization schema for service requests to network functions based on OAuth 2.0 framework. NRF (Network Repository Function) acting as OAuth authorization server, authorizes NFs for using services provided by other NFs, exposed by APIs, according to predefined policies.

In addition, new service communication models have been introduced between consumers and producers in SBA. Specifically, a new component named as SCP (Service Communication Proxy) enables indirect communication for NF-NF interactions, acting as a trusted intermediary with certain delegated functions. SCP can assume functions of services discovery and selection of instances providing those services on behalf of the consumer, as well as routing functions. In addition, a concept of Client Credentials Assertions (CCA) has been added, to enable end to end authentication by signed tokens in NF consumer side. These mechanisms enable the support of service mesh architectures.

5) Enhancements for Interconnection Security: 5G system introduces a new entity named SEPP (Security Edge Protection Proxy) for signalling interconnection between operators. All roaming control traffic is routed via the SEPP and the N32 interface to the SEPP of the other PLMN. Two protection mechanisms have been specified, TLS at network layer, and PRINS (PRotocol for N32 INterconnect Security) at application layer for JSON (Java Script Object Notation) information elements on N32. The SEPPs have the capability of security negotiations, i.e., selecting the protection mechanism, and in case of PRINS applying granularly encryption, integrity protection and authentication at information element level.

6) Non-Public Networks (NPN) Security: A NPN is a 5G system deployed for non-public use. It comes in two flavours, standalone NPN (SNPN) and Public Network integrated NPN (PNiNPN). SNPN is operated by an NPN operator not relaying on operator functions provided by a PLMN, whereas a PNiNPN is deployed with the support of a PLMN. Most of the security procedures are exactly the same in NPN as in public networks, with small deviations introduced in annex I of [15]. Note that for SNPN, in addition to 3GPP defined authentication mechanisms (i.e., 5G AKA and EAP-AKA'), additional methods are possible (e.g., EAP-TLS).

7) Wireline Wireless Convergence (WWC) to 5G Core Security Aspects: WWC adds trusted access to 5G core from other non-3GPP access networks such as wireline networks. Two new entities are added in the architecture, 5G-RG (5G Residential Gateway) and FN-RG (Fixed Network Residential Gateway). 5G-RG acts as a 5G UE and can connect to 5G Core via wireline access network (W-5GAN) or via Fixed Wireless Access (FWA). FN-RG connects to 5G Core via W-5GAN. The authentication for trusted non-3GPP access is similar to untrusted authentication using N3IWF (Non-3GPP access InterWorking Function).

The areas of security best practices, security operations and security assurance schemas are as mentioned relevant in a comprehensive security framework deployed for a 5G network, but out of the scope of the article.

C. ITS-5G Security Enhancement

The following security features are network-native, however they expand to the application layer, so that the ITS system is aware of such features and exchanges information with the network for secondary authentication and interface protection, see Fig. 5(b).

1) EAP-Based Secondary Authentication, and Slice Specific Authentication and Authorization: Secondary authentication is a mechanism by which a UE and an external entity (typically Authorization and Authentication - AA server) can authenticate each other after the (primary) authentication between UE and 5G system has occurred. The EAP framework specified in RFC 3748 was selected for that purpose. This is done for trusted services, which may be offered by the MNO (in this case the AA server is at the network premises) or by trusted providers such as the ones that agree a network slice for its customers. In this case, the AA server may be not at the network premises. This will be, most probably, the case of ITS systems.

A new function named as NSSAF (Network Slice Authentication and Authorization Function) has been created in 5G for interaction with 3rd party AA servers. An authorized slice identified by S-NSSAI (Single - Network Selection Assistance Information) is granted to a UE after the UE has successfully completed the primary authentication (between UE and 5G). Network slice-specific authentication and authorization uses a User ID and credentials, different from the 3GPP subscription credentials, and EAP framework is defined for those mechanisms by the Slice tenant (ITS system).

2) Authentication and Key Management for Applications (AKMA): AKMA is a new delegated authentication system of 5G [20], specified in [21]. This feature introduces third party application specific authentication, key derivation and bootstrapping based on PLMN generated session key. That way, operators are enabled to monetize key management services for 3rd party entities such as verticals using their subscription. AKMA is thought for service providers that are not trusted (e.g., they do not agree the use of a network slice) but that want to use enhanced authentication using PLMN authentication and authorization as the basis. This would be the case of an ITS system that renounces to use network slice.

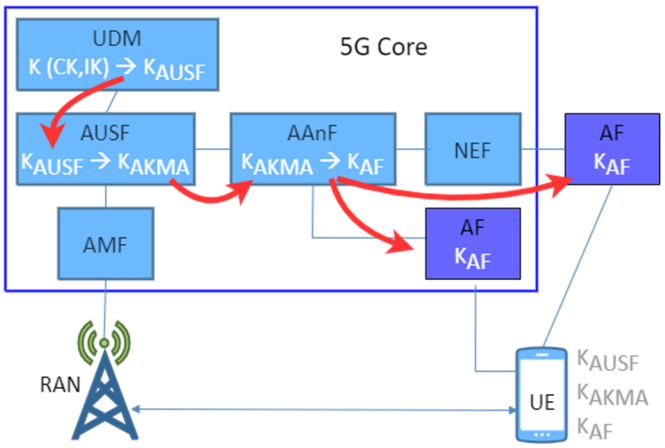

Fig. 9. Simplified block diagram and key generation of AKMA. AMF- Access and mobility management function; UDM- Unified data management function; AUSF- Authentication server function; AAnF- AKMA anchor function; NEF- network expousure function; AF- Application function.

In AKMA, the application specific key is derived from the key generated for primary authentication of the UE [21].

AKMA requires a new logical entity known as AKMA Anchor Function (AAnF), placed in the HPLMN (Home PLMN) to generate the key material to be used between the UE and the Application Function (AF), maintaining the UE AKMA contexts. The AF is owned by the Third Party that receives the Key K_{AF} from the AAnF at the network side, see Fig. 9. The AF and the AAnF may be directly connected or through the Network Exposure Function (NEF). The K_{AF} is also generated in the UE when the UE is notified from the network that AKMA is in course. Then, AF and UE may authenticate by using the K_{AF}.

At the network side the K_{AF} is derived in the AAnF from the K_{AKMA} received from the AUSF (Authentication Server Function), who, in its turn, derived K_{AKMA} from the K_{AUSF} (the K_{AUSF} is derived from the subscriber's key K stored in the Unified Data Management Function, UDM). The following diagram summarizes the main building blocks and key generation of AKMA.

3) Vehicle to Everything Services (V2X) Security Aspects: V2X architecture defined by 3GPP supports V2X (Vehicle-To-Everything) 5G-based communications over both (1) the Uu reference point between the UE and NG-RAN (Next Generation-Radio Access Network, which includes 4G base station adapted to 5G Core and 5G New Radio base station) and (2) the PC5 reference point (between two or more UEs). NR (New Radio) based PC5 reference point supports unicast, groupcast and broadcast modes, see Fig. 4. There have defined in [22] a list of security requirements for securing the PC5 unicast link, which uses 4 different layers of keying material:

- Long term credentials: credentials that are provisioned into the UE(s) and form the root of the security of the PC5 unicast link;
- KNRP: 256-bit key that is shared between the two entities communicating using NR PC5 unicast link;
- KNRP-sess: 256-bit key that is the root of the actual security context between the UEs. Confidentiality and

Integrity Keys are derived from KNRP-sess. The 16-bit KNRP-sess ID identifies the KNRP-sess;

- NRPEK and NRPIK: NR PC5 Encryption Key (NRPEK) and NR PC5 Integrity Key (NRPIK) are used for protecting PC5-S signaling, PC5 RRC signaling, and PC5 user plane data.

There are not special requirements or security procedures for securing PC5 for groupcast/broadcast modes, since it is assumed that that information should be unciphered.

There are not additional or specific requirements for securing V2X over Uu reference point beyond those given in [15] for Uu connectivity with 5G Core network.

4) CIoT (Cellular IoT) Security Enhancements: CIoT is used in applications where the users exchange small data such as SMS (Short Message Signaling). This is the case in some application used in transportation systems. In CIoT, security may be handled in control plane (CP) as payload of a protected NAS (Non Access Stratum) message in both UL/DL (Uplink/Downlink).

In the case that user data are sent through the UP (User Plane), then CIoT transmissions are allowed to suspend an RRC (Radio Resource Control) connection in the NG-RAN, to be resumed by the UE using the connection at a later time. For CIoT transmissions, there is also protection of Non-IP Data Delivery (NIDD) in the interface between NEF (Network Exposure Function) and external AF (Application Function). CIoT may be used by the ITS-S for short messaging if available.

D. Secure Infrastructure

The last vast domain where security must be assured is the underlying infrastructure.

The concept of decoupling the 5G network functions and applications from the infrastructure becomes a challenge for designing a sound end-to-end security architecture. The infrastructure needs to support not only the secure performance of the 5G system, but also the specific requirements of the potential tenants enabled by network slicing, and specific regulatory demands. Fig.10 provides a basic representation of the multi-layer architecture in a data centre, pointing out the corresponding security areas:

The adoption of these new network paradigms increases the potential attack surface, as new entities are included in the 'telco' architecture to support the 5G system. Building a trusted secure infrastructure hosting the 5G system requires a holistic approach including multiple security controls across all layers mentioned above. In this section a non-exhaustive key list of those security controls is provided, highlighting the rationale of implementing them in 'telco' cloud infrastructures for verticals such as ITS.

1) Network Function Virtualization (NFV): New network paradigms and technologies are adopted to host and connect 5G networks, such as NFV (Network Function Virtualization), that constitute an essential part of what the industry generally denominates 'telco' infrastructure. In the context of a 3GPP network, NFV refers to the deployment of Network Functions (NFs) as software modules which run on off-the-shelf computing hardware. As most of NFs run in NFV

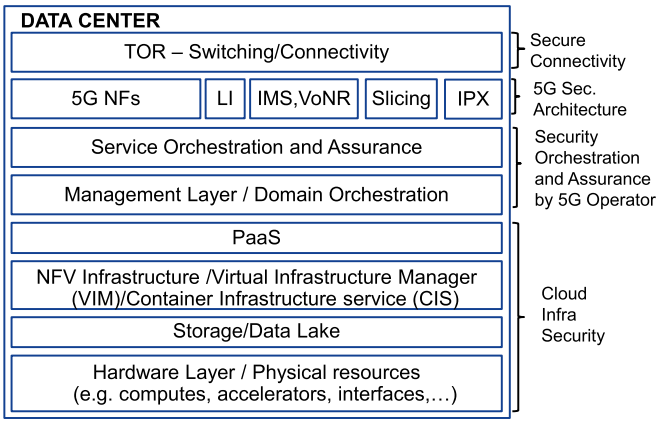

Fig. 10. Multi-layer architecture in a data center.

platforms, and indeed the implementation of the 5G Service Based Architecture relies on the use of NFV (among other technologies), NFV security mechanisms are a cornerstone of the overall 5G network security architecture.

European Telecommunication Standard Institute (ETSI) Industry Specification Group (ISG) for NFV defines multiple aspects related to the infrastructure supporting 5G networks, such as virtualization techniques (virtual machines, containers), operational processes, management, security and orchestration.

Those technologies are being deployed on cloud environments (private, public or hybrid), typically implemented in highly distributed architectures of data centres (i.e., edge, regional and/or central clouds).

2) Cloud Security Assurance: Security by design principles must be considered from the initial phases of every product design and creation, through the implementation until maintenance and finally de-commissioning, in short during the whole product lifecycle. Cloud products include among others: physical hosts, virtualization platform software (e.g., NFV, CIS), Virtual Network Functions (VNFs) and Management functions (e.g., VIM). X86 and similar server architectures have a number of physical security weaknesses from a critical national infrastructure perspective, which represent a risk to the 3GPP security architecture [23]. Therefore, physically securing all hosts building the cloud infrastructure is needed, although also difficult to achieve. The cloud stack needs to be robust and protected against malicious application software with access to the platform via application programming interfaces (APIs). On the other side, an attacker with root access to the virtualization layer in the administration domain can gain access to the VNFs and view and edit the memory of those [23]. Therefore, well-established security practices like secure coding, hardening, security testing and auditing, need to be correspondingly adapted and applied to the entire cloud ecosystem.

3) System Integrity: Depending on the host environment and use cases under consideration, stronger trust in the integrity of a particular deployment than provided by the cloud stack may need to be established. Trusted Platform Modules (TPM) working as Hardware-Based Root of

Trust (HBRT), can ensure the integrity of the software (e.g., NFV platform) at boot time. The HBRT is meant to support a secure boot as well as a highly secure management of cryptography keys (key generation, key storage) and execution of crypto operations making use of the securely stored keys. Later, the integrity of the software can be achieved by remote attestation mechanisms. To attest a virtualized 3GPP NF through a full chain of trust from the VNF layer down to the hardware layer, an attestation infrastructure and procedures are needed within the 3GPP domain and outside of it. VNFs and applications images also need to be integrity protected in order to prevent an attacker to tamper.

4) Isolation & Traffic Separation and Security Zones: Both are well-known security mechanisms to be applied to cloud environments, typically deployed in shared physical infrastructures to allow to scale services up and down as required, and to centralize the management and orchestration. Highly sensitive cases may require the implementation of physical separation, that can be achieved by for example assigning dedicated physical resources to specific VNFs or interfaces managing specific types of traffic. Nevertheless, in most of the cases a logical separation can achieve an acceptable level of security and prevent side-channel attacks.

Virtual Machine (VM) based virtualization is being migrated towards Container based virtualization, what clearly brings benefits in terms of flexibility, efficiency and agility in the architecture, but from security viewpoint, and concretely looking at the isolation aspects of it, represents a serious challenge. The VM hypervisor is replaced by a container engine which manages the lifecycle of a container within a group (pod or cluster). However, the container engine does not provide equivalent VM security memory isolation. Therefore, conscious decisions need to be made during the design phase to establish appropriate restrictions on container placement (e.g., separation of containers belonging to different NFs on different physical servers), which of course can decrease the desired agility and flexibility of the architecture.

Different types of traffic, such as control plane traffic, user plane traffic, O&M (Operation and Maintenance) traffic or synchronization traffic are typically created and isolated by VLANs/VXLANs (Virtual/Extended Local Area Networks) and VPNs (Virtual Private Networks), which can be implemented by physical and/or virtual switching/networking/security devices part of the infrastructure (e.g., virtual switches, virtual routers, virtual firewalls, etc.). Network segmentation in different security zones, so called trust domains, can be as well implemented by that infrastructure, based on predetermined shared security requirements and policies per zone/domain. All workloads, functions and VNFs should be allocated to a trust domain, based upon those requirements and policies. For example, critical and sensitive workloads (e.g., working with secrets or subscriber data) should not run on the same host pool than highly exposed workloads (e.g., proxies).

5) Confidentiality Protection: Several cryptographic mechanisms have been described earlier to protect the confidentiality of 3GPP 5G reference points. However, there are multiple interfaces in the infrastructure as well as critical entities storing sensitive data (e.g., keys, shared secrets, etc.), for whom confidentiality protection mechanisms have not been standardized. The cloud infrastructure needs to provide such mechanisms where it is needed, for both data in transit and at rest.

6) Secure Operations and Management: The operation and management (including security) of the infrastructure is crucial to be performed with a high grade of automation, required by 5G networks due to the dynamic nature of the service based oriented architecture and new network paradigms such as Network Slicing and consequent multi-tenancy considerations. The set of automated operation and management procedures compose the term of service orchestration. Securing the service orchestration in the infrastructure comprises multiple technologies related to access control (e.g., privilege access management, attribute-based access control, etc.), security monitoring (e.g., Intrusion Detection Systems, Security Incident and Event Management, etc.), self-adaptive and automatic security mechanisms governed by SOAR (Security Orchestration, automation and response) type of platforms and others.

Security functionalities of the physical infrastructure should demonstrate the capacity to protect the infrastructure in order that the network may be securely implemented on it. Security assurance of the physical platform is normally done at a time T_0 different to security assurance of the network and ITS layer. Therefore, composite or multi-assurance composite will be operated for the integration of the physical infrastructure and the network.

V. Example Security Assurance of 5G Supporting ITS Connectivity

Under the light of the ITS-on-5G context of the previous section, an ITS customer (e.g., cars or trucks manufacturer) will put requirements to the security of the network and underlying infrastructure that needs to be comprehensively demonstrated in the whole system.

The strategy for selecting the sub-systems presented in Section III shows the necessity that all the attributes are comparable. In the case of EAL attributes, the selected reference level that separates the attribute classification in unacceptable or acceptable, needs to be the same in all attributes, i.e., in all the evaluations of the sub-systems.

This means that the evaluation provided into the sub-systems should follow a comprehensive testing methodology that shows that all the sub-systems have the same level of security protection against external attacks. The comprehensive evaluation methodology imposes also the same evaluation criteria, which define general principles how to perform the evaluation for each of the EAL concerned, and what requirements must be met in order to obtain a PASS evaluation result. Regretfully, the evaluation of each sub-system follows different evaluation/certification schemes.

In this section, we discuss the different standards for security assurance at different layers (automation, network and underlying) and argue that commercial security assurance schemes at the network layer lack of flexibility due to the fact that they offer only one level of security assurance (sub-section A). The sub-section B presents example results of how

multiple security assurance levels could be conducted on the network components (e.g., network functions). More levels of security assurance make feasible the selection of proper implementation (of 5G network) by considering the intended use in the automotive systems.

A. Current Evaluation Schemes at Different Layers

At the **automotive vertical layer**, the Electronic Control Units (ECUs) must be well protected and the data processing within the car must be resistant to external and internal attacks. The hardware of the ECUs, including communication ECUs, rely on certification schemes that evaluate the protection of the information assets for data processing. In order to ensure security and safety in their ECUs, vehicle manufacturers have to meet different regulations and standards. Concerning the Cyber Security Management System (CSMS), the ISO 21434 standard [38] specifies engineering requirements for cybersecurity risk management of electrical and electronic systems in road vehicles. It defines a framework and a common language for the entire supply chain and for the entire vehicle lifecycle (concept, product development, production, operation, maintenance and decommissioning). However, specific cybersecurity technologies, solutions and requirements are not included. It is a risk-oriented approach, where the TARA methodology (Threat Analysis and Risk Assessment) is considered, to identify and classify assets and threat scenarios, and to do a risk value determination and a risk treatment decision. Related to this ISO standard, other regulations exist that must be taken into account in some countries, such as the UNECE R155 regulation [40], which must be complied by all vehicles manufactured in the European Union from 2021 to get their Certificate of Compliance for Cyber Security Management System.

Specific regulation or market requirements introduce evaluation (or certification) schemes in order to provide assurance that the hardware and software in the automotive industry is compliant with the standards. An often-used scheme is Common Criteria (CC), which is a certification scheme that aims to achieve widest available mutual (among countries belonging to Common Criteria Recognition Arrangement) recognition of security of IT products. The device producers describe the Security Functionalities of the product with a list of Security Functionality Requirements (SFR) by following the CC standard. Moreover, they claim the required EAL level, which is the basis for the laboratory to define the Security Assurance Requirements (SAR) with the description of the evaluation tasks. The SARs contains the following Assurance Classes related with evaluation activities: Security Target Evaluation, (product), Development, Guidance Documents, Life-cycle support, Tests and Vulnerability Assessment. After evaluating the product, the laboratory issues a report that will be the basis of the certification of the product.

One of the main problems of any certification scheme is how to manage software updates. Common Criteria proposes to evaluate the software in the first release and to follow the parts that will be updated, reducing the evaluation costs of future releases. The problem of software updates evaluation and continuous compliance assessment requires a high discussion and is out of the scope of this paper. However, let us remark that this problem is very sensitive in automation and it is actually under research. ISO has recently published its standard ISO 24089 [39], and there is also a UNECE regulation, R156 [41]. In these documents, the emphasis is on the Software Update Management System (SUMS), with special focus on OTA (Over-the-air) updates.

At the **network level**, security and security assurance are based on the concept of security-by-design, which means that the design for security principles are to be enforced in the creation of each component across its entire lifecycle (e.g., secure coding, hardening, security testing, security vulnerability monitoring, etc.). 3GPP has published a series of security assurance specifications known as 5G Security Assurance Specification (SCAS) (e.g., TS 33.511 for gNB [43]), which list the security requirements and corresponding test use cases per 5G NF. These technical specifications are used in security industry schemas like GSMA NESAS [24], created to evaluate the security posture of vendors in terms of development processes and supplied products. The evaluation methodology is well defined in SCAS documents and includes port scanning (which ports of the external interface respond to requests), vulnerability scanning (if the products have known vulnerabilities) and interface robustness and fuzz testing. Other penetration tests and peer-review tests are not considered in GSMA NESAS. Different levels of network security assurance are not demonstrable in NESAS.

At the **underlying infrastructure**, the most important evaluation schemes are directed to demonstrate security protection of clouds. Securing the 5G cloud infrastructure is being addressed not only by the industry and associated standardization organization, but also by regulators and agencies working for Governments around the globe. National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) have published in 2021 four-part series of security guidance for 5G cloud infrastructures [25], addressing different aspects such as prevention and detection of lateral movements (part I), isolation of network resources (part II), data protection in transit, in use, and at rest (part III) and integrity assurance of the infrastructure (part IV). The best practices of this series of documents are oriented to new Zero Trust Architecture (ZTA) principles as defined in [17]. The European Union Agency for Cybersecurity (ENISA) has recently published a report [26], which explores the challenges, vulnerabilities and attacks to NFV within the 5G network, and also provides a guidance of security control and best practices to cope with them. Among the main challenges described by ENISA are the following: increase of attack surface due to use of standardized general-purpose server and storage machines routinely built with open-source code, growing participation of multiple stakeholders and complex supply chains, more software components, and decentralization of the 5G NFV architecture in multiple clouds (central, edge). To solve those challenges some of the key best practices proposed in the report are the following: applying security-by-design across all 5G NFV network elements and layers, security management and orchestration to coordinate the

security protection across all layers, hardening and patching the NFV infrastructure, applying isolation principles, encryption, identity management, etc.

B. Example Security Assurance at Different Levels for Network Equipment: The N4 Interface

In this sub-section, we aim to demonstrate that it is possible to evaluate 5G network equipment at different levels of security assurance. Concretely, we perform evaluation tests at three different security assurance levels of one example interface of the 5G network that is crucial for the ITS system: the N4 interface between the SMF (Session Management Function) and the UPF (User Plane Function). These example tests aim to show the different assurance levels that 5G network could demonstrate in order to fulfil security requirements of the ITS customer that will make use of the network for connectivity service. In this case, as discussed in Section II, it is important to consider that different components may have been evaluated at different levels of security assurance, and their use in the same system may pose challenges when ensuring the requested security assurance level for the whole system. Therefore, the borders of the system need to be well defined when implementing the security controls of the different layers.

The N4 interface transports signalling related to the session management between the SMF and the UPF. For example, it is sent all the information about QoS requirements, security requirements of the session transport (tunnelling), policies about user's session data forwarding, and so on. The N4 interface is a non-SBA (Software Based Architecture) interface, so it requires that security is enforced point-to-point. It is an internal 5G Core interface and, as all internal interfaces, may transport signalling data as well as privacy sensitive material (e.g., user and subscription data, or others such as security keys) [27], therefore, confidentiality and integrity protection are required. The standard for the N4 interface security is defined in ETSI TS 133 513: "5G Security Assurance Specification (SCAS); User Plane Function (UPF)". The main security requirements for the N4 is to create a Network Domain Security (NDS) by enforcing IP network layer security. This way, signalling data (in N4 there are not user data) will remain confidential and their integration will be protected.

In our evaluation tests we discuss three different levels of security assurance, called low, medium and high for the purposes of this paper.

The level low will consider only the analysis of the security standards of the tested interface and whether the network equipment under test (Target of Evaluation, TOE) is compliant with the security standard (e.g., the required security protocols are running properly).

The medium level evaluation tests will include the analysis of known vulnerabilities of the security mechanisms working on the interface and whether our TOE is protected against attacks to such vulnerabilities. These tests will require a tool for trying to attack the interface through the known vulnerabilities.

The third level (high) of network assurance will require advanced knowledge on the interface, in order to analyse the content of the messages against what can be considered a normal network behaviour. In these tests we will aim to break the security of the interface by providing some changes to the normal communication between the Network Functions. The objective of the tests is to check if the Network Function responds anomaly to any of the unnormal messages.

The three levels of network assurance are directly related with the efforts and knowledge that the tester needs to put for evaluating the TOE. It is worth to remark than this effort is also related with the effort that an attacker will need to do for hacking the system. So, the security protects the system against a given level of means (knowledge and tools) of the attacker.

In our tests the name of the producer of the TOE will remain reserved.

TABLE I
LOW ASSURANCE TESTS OF N4 INTERFACE

Test No.	Sec. Ass. Level	Name test	Vulnerability	**Test result**
#1	Low	IPSec tunnel active?	None	**Pass**
#2	Low	Fake secure conn. UPF-SMF?	None	**Pass**

C. Low Security Assurance Level. The Tests Provided at the Lowest Level of Security Assurance Are as Follows

- To analyze security standards of the N4 interface;
- To check whether the TOE has activated all the security mechanisms and they are running properly.

The analysis of the security standards is defined in ETSI TS 133 513 (UPF), ETSI TS 133.501 (Non-SBA interfaces) and TS 133 210 (Network Domain Security). The latter standard specifies the security mechanisms that should be enforced. The security in N4 is based on IPSec and TLS, and the key management and key distribution by the protocol Internet Key Exchange version 2 (IKEv2).

In order to check the real implementation of the security protocols in our TOE, we connected the SMF and UPF as in real environment, but we reserved access to the interface. In our scenario, the tunnel mode IPsec ESP and IKEv2 certificate authentication are implemented (as suggested in [28]). With this security implemented, we gain access to the UPF through the Operations & Maintenance (O&M) connection and check whether tunnelling is properly executed, including all the versions of the certificate authentication. Moreover, as suggested in [29, clause 4.2.3.2.4], we try to establish a secure connection between UPF and SMF when the IKE has not been activated. For this last test, the expected result is that it is not possible to have a secure combination between the NFs.

Our TOE passed both tests positively, as shown in Table I.

There are many other potential tests to do. SCAS specifies at least one more test on this interface related with the GPRS Tunnelling Protocol [28, clause 4.2.2.6], however, for the scope of this example, we only tested IPSec in the interface.

1) Medium Security Assurance Level: The tests provided at the medium level of security assurance include checking whether known vulnerabilities of the security protocols used in the N4 interface are present in our TOE. For this, we make use

TABLE II
MEDIUM ASSURANCE TESTS OF N4 INTERFACE

Test No.	Sec. Ass. Level	Name test	Vulnerability	**Test result**
#3	Medium	pluto IKE daemon restart?	CVE-2019-12312	**Pass**
#4	Medium	daemon restart?	CVE-2016-3071	**Pass**
#5	Medium	DoS_restart?	CVE-2013-7294	**Pass**
#6	Medium	DoS_expected_payload	CVE-2013-6467	**Pass**
#7	Medium	secret hash leakage?	EDB-ID: 22532	**Pass**
#8	Medium	Missing DLL	EDB-ID: 28130	**Pass**
#9	Medium	Bruteforce IKEv2 IPSec	hacktricks/IPSec/IKE	**Pass**

of different databases with known vulnerabilities of IPSec and IKEv2. In [30] we may find 175 vulnerabilities for IPSec and 39 for IKEv2 (date: 15.06.2022). We search the vulnerabilities that may appear in our TOE by checking the libraries of IPSec and IKEv2 that our TOE uses. From the whole list it seems that only four IKEv2 vulnerabilities could appear in our TOE, however the version of the library installed in the TOE is newer than the versions containing vulnerabilities in CVE list, so most probably, these vulnerabilities do not appear in our TOE. However, we provided the tests on those vulnerabilities and, as expected, the result was negative (these known vulnerabilities do not appear in our TOE), as shown in Table II. In addition, we provided other two tests based on exploit database [31], concretely there are two potential vulnerabilities that needed to be checked in our TOE: the first one is related with IKE and AuthIP IPsec Keyring Modules Service and consists of a potential missing DLL [32], and the second one is a potential shared secret hash leakage when using IKEv2 [33]. The hacker exploiting software is available in the above-mentioned pages. By testing the TOE with that software, we observed that the vulnerabilities were not exploited since the responses of the TOE were that the requests are unknown, as shown in Table II.

We conducted a last test on known vulnerabilities by using the pentesting tool in [34]. These tools aim to bruteforce security information in the TOE by overflooding the interface with requests for bidding down security in the IPSec tunnel. A reservation of processing power for security tasks avoids any vulnerability to that kind of attack. Without vulnerabilities, the system will not respond positively to the requests and, most probably, the system will collapse due to the continued overflooding of signaling messages. If there is a vulnerability, then the system could accept reducing security in order to save the processor. Fig. 11 presents the values of processor occupancy for increasing number of requests. We repeated the test three times by increasing the time of bruteforcing each sample (e.g., 200 requests/s are sent during 1, 4 and 10 seconds, respectively). We are repeating the tests for different time stamps since the TOE could behave differently whether the overload is instantaneous or long-term. As we can see in Fig. 11 it is not the case of our TOE, which behaves almost identically regardless of the time of signaling bruteforcing.

The results confirm that the processor gets overflooding with around 900 requests/s, where the UPF crashes and must be restarted, however in any case the UPF did not responded affirmatively to the requests, so we may confirm that the TOE does not contain vulnerability in the reservation of resources

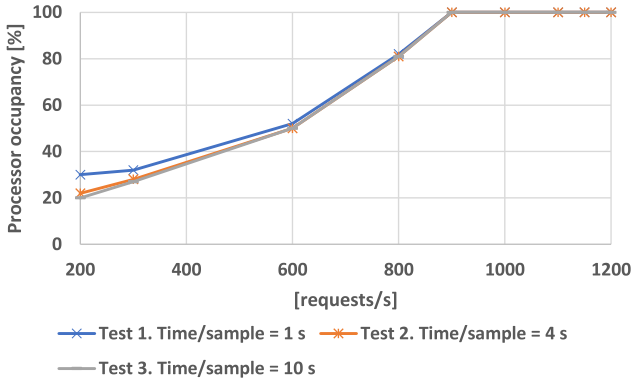

Fig. 11. Processor occupancy for increasing number of security bidding-down.

for security tasks. The fact that the TOE crashes could be seen as an attack to availability but in these tests (as normally it is done during security evaluation) we are only evaluating confidentiality and integrity protection.

The conclusion is that the TOE has passed the test positively as pointed out in Table II.

2) High Security Assurance Level: The tests provided at the high level of security assurance are more specific to the specification of the TOE functionalities. For this example, we provide a tampering attack to the UPF.

UPF forwards packets to/from the gNB (5G base station) based on GPRS Tunneling Protocol for User data (GTP-U) tunneling. GTP-U tunnels are assigned when a new user data flow is starting. The identifier of the GTP tunnel (called Traffic Endpoint Identifier, TEID) is assigned by the receiver (the receiver end point of the tunnel) and passed to the sender before the data transmission. At the receiving point, the packets that contain unrecognized TEID are discarded.

The communication between SMF and UPF (N4 interface) is done by the Packet Forwarding Control Protocol (PFCP) that also uses TEID labels for classifying the traffic in different tunnels. Normally, the UPF should maintain the GTP-U tunnels (with the gNB) and the PFCP associations (with the SMF) in different domains (i.e., different processing space such as different pods, and different memory spaces). In this case, cornering all the sessions of PFCP will not have any impact to labeling of GTP-U tunnels. However, it is possible that the TEID labels are kept in the same memory space so PFCP sessions contexts and GTP-U TEIDs are not independent.

Our attack will consist of opening many PFCP session contexts between SMF and UPF in order to corner all the potential TEID labels. In the case, that PCFP and GTP-U labels are not independent, then this could interrupt the routing of new traffic between gNB and UPF. This would mean that the UPF has a vulnerability in the treatment of PCFP sessions and GTP-u tunnels in N4 and N3 interfaces, respectively.

The steps of the attack are:

1. Connecting the UPF to SMF through N4 interface and connecting the UPF and gNB through N3 interface;
2. Initiating a connection of one user to the gNB (Non-Access Stratum and Access Stratum signaling);

TABLE III
HIGH ASSURANCE TESTS OF N4 INTERFACE

Test No.	Sec. Ass. Level	Name test	Vulnerability	**Test result**
#10	High	Tampering GTP U tunnels	TEID lab not-isolated	**Pass**

3. Sending GTP tunnel requests from SMF to UPF (N4 interface). As the TEID are up to 4 octets long, then the number of requests should be at least 2^{32}. Then all the GTP channels between the UPF and the SMF should be occupied;
4. Initiating a data session from the user to the Internet. If the session is established, then we assume that the TOE (UPF) is working properly since a new different TEID is assigned to that traffic. If the session cannot be established, then it is possible (it should be further confirmed) that the vulnerability exists in the TOE.

As we can see in Table III, the result of the test is positive and the vulnerability does not exist (the user's data session was properly established even if the GTP tunnels between SMF and UPF were saturated).

VI. CONCLUSION

The tests performed above are only example evaluation and does not provide a complete and standard evaluation. Obviously, a real evaluation is done in a much more sophisticated way and with the use of sophisticated tools. However, the analysis provided in this paper together with the example security assurance at different levels provide to the following conclusions:

- ITS customers (and, in general, any business using networks) may apply a strategy that follows *multicriteria decision making* for selecting the ICT sub-system based on security requirements;
- The assurance of end-to-end security is based on a set of security functionalities that span from ITS layer to 5G network and physical underlying infrastructure;
- A comprehensive evaluation methodology is required through all the certification/evaluation schemes of different sub-systems;
- End-to-end enhanced security requires integration of the ICT sub-systems. Such an integration may be achieved through the exchange of security key vectors made available through secured interfaces;
- Currently, the diversity of certification schemes and evaluation methodologies makes difficult that a complex system may unambiguously demonstrate security protection.

REFERENCES

[1] *Information Technology—Security Techniques—Evaluation Criteria for IT Security—Part 1: Introduction and General Model*, Standard ISO/IEC 15408-1:2009, 2015

[2] (May 2018). *SOG-IS Joint Interpretation Library, Composite Product Evaluation for Smart Cards and Similar Devices*. Accessed: Jun. 2022. [Online]. Available: https://www.sogis.eu/documents/cc/domains/sc/JIL-Composite-product-evaluation-for-Smart-Cards-and-similar-devices-v1.5.1.pdf

[3] *Common Criteria Certified Products*. Accessed: Jun. 2022. [Online]. Available: https://www.commoncriteriaportal.org/products/

[4] *Information Security, Cybersecurity and Privacy Protection—New Concepts and Changes in ISO/IEC 15408:2022 and ISO/IEC 18045:2022*, Standard ISO/IEC TR 22216:2022, 2022

[5] D. Jiang, L. Huo, Z. Lv, H. Song, and W. Qin, "A joint multi-criteria utility-based network selection approach for vehicle-to-infrastructure networking," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 10, pp. 3305–3319, Oct. 2018, doi: 10.1109/TITS.2017.2778939.

[6] G. Pal, K. Atkinson, and G. Li, "Managing heterogeneous data on a big data platform: A multi-criteria decision making model for data-intensive science," in *Proc. IEEE Int. Conf. Big Data Smart Comput. (BigComp)*, Feb. 2020, pp. 229–239, doi: 10.1109/BigComp48618.2020.00-69.

[7] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 11, pp. 2898–2915, Nov. 2017, doi: 10.1109/TITS.2017.2665968.

[8] *Intelligent Transport Systems (ITS); Communications Architecture*, Standard ETSI EN 302 665, Sep. 2010.

[9] *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*, Standard ETSI EN 302 637-2, Apr. 2019.

[10] *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specification of Decentralized Environmental Basic Service*, Standard ETSI EN 302 637-3, Apr. 2019.

[11] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960–969, Apr. 2016, doi: 10.1109/TITS.2015.2494017.

[12] *Intelligent Transport Systems (ITS); Security; Security Services and Architecture*, Standard ETSI TS 102 731, Sep. 2010.

[13] *Intelligent Transport Systems (ITS); Security; ITS Communications Security Architecture and Security Management*, Standard ETSI TS 102 940, Jul. 2021.

[14] *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; Release 2*, Standard ETSI TS 102 941, Oct. 2021.

[15] *Security Architecture and Procedures for 5G System (Release 17)*, document TS 33.501, 3GPP, 2023.

[16] D. Chandramouli, R. Liebhart, and J. Pirskanen, Eds., *5G for the Connected World*, 1st ed. Hoboken, NJ, USA: Wiley, 2019.

[17] NIST. (Aug. 2020). *Zero Trust Architecture*. [Online]. Available: https://www.nist.gov/publications/zero-trust-architecture

[18] *Management and Orchestration; Generic Management Services' (Release 17)*, document TS 28.532, 3GPP, 2023.

[19] NOKIA Bell Labs Institute. (Oct. 2021). *A Comparison of 4G and 5G Authentication Methods*. [Online]. Available: https://www.bell-labs.com/institute/publications/a-comparison-of-4g-and-5g-authentication-methods/#gref

[20] M. Khan, P. Ginzboorg, and V. Niemi, "AKMA: Delegated authentication system of 5G," *IEEE Commun. Standards Mag.*, vol. 5, no. 3, pp. 56–61, Sep. 2021, doi: 10.1109/MCOMSTD.101.2100015.

[21] *Authentication and Key Management for Applications (AKMA) Based on 3GPP Credentials in the 5G System (5GS)*, document TS 33.535, 3GPP, 2023.

[22] *Security Aspects of 3GPP Support for Advanced Vehicle-to-Everything (V2X) Services*, document TS 33.536, 3GPP, 2022.

[23] *Study on Security Impacts of Virtualization (Release 17)*, document TR 33.848, 3GPP, 2023. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3574

[24] *GSMA Network Equipment Security Assurance Scheme (NESAS)*. Accessed: Oct. 2023. [Online]. Available: https://www.gsma.com/security/network-equipment-security-assurance-scheme/

[25] *Security Guidance for 5G Cloud Infrastructures Parts I, II, III, IV*, Nat. Secur. Agency (NSA), Cyber Secur. Infrastruct. Secur. Agency (CISA), Fort Meade, MD, USA, 2021. Accessed: Oct. 2023. [Online]. Available: https://www.cisa.gov/resources-tools/resources/security-guidance-5g-cloud-infrastructures

[26] *NFV Security in 5G—Challenges and Best Practices*, Eur. Union Agency Cybersecur. (ENISA), Attica, Greece, Feb. 2022.

[27] *Security Architecture and Procedures for 5G System*, document ETSI TS 133 501 V16.3.0, Aug. 2020.

[28] *5G Security Assurance Specification (SCAS); User Plane Function (UPF)*, document ETSI TS 133 513 V16.1.0, Oct. 2020.

[29] *Catalogue of General Security Assurance Requirements*, document ETSI TS 133 117 V15.2.0, Apr. 2019.

[30] *CVE Program*. Accessed: Jun. 2022. [Online]. Available: https://cve.mitre.org/
[31] *Exploit Database*. Accessed: Jun. 2022. [Online]. Available: https://www.exploit-db.com/
[32] *Exploit Database: IKE and AuthIP IPsec Keyring Modules Service (IKEEXT)—Missing DLL (Metasploit)*. Accessed: Jun. 2022. [Online]. Available: https://www.exploit-db.com/exploits/28130
[33] *Exploit Database: IKE—Aggressive Mode Shared Secret Hash Leakage*. Accessed: Jun. 2022. [Online]. Available: https://www.exploit-db.com/exploits/22532
[34] *HackTricks: 500/UDP—Pentesting IPsec/IKE VPN*. Accessed: Jun. 2022. [Online]. Available: https://book.hacktricks.xyz/network-services-pentesting/ipsec-ike-vpn-pentesting
[35] *IEEE Standard for Information Technology-Local and Metropolitan Area Networks. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11-2012, Mar. 2012.
[36] *Intelligent Transport Systems (ITS); ITS-G5 Access Layer Specification for Intelligent Transport Systems Operating in the 5 GHz Frequency Band*, document ETSI EN 302 663 V1.3.1, Jan. 2020.
[37] *IEEE Approved Draft Standard for Information Technology—Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Next Generation V2X*, Standard IEEE P802.11bd/D8.0, Dec. 2022, pp. 1–148.
[38] *Road Vehicles—Cybersecurity Engineering*, Standard ISO/SAE 21434, Aug. 2021.
[39] *Road Vehicles—Software Update Engineering*, Standard ISO/SAE 24089, Feb. 2023.
[40] *E/ECE/TRANS/505/Rev.3/Add.154—UN Regulation No. 155—Cyber Security and Cyber Security Management System*, United Nations Economic Commission for Europe (UNECE), Geneva, Switzerland, Mar. 2021.
[41] *E/ECE/TRANS/505/Rev.3/Add.155—UN Regulation No. 156,—Software Update and Software Update Management System*, United Nations Economic Commission Europe (UNECE), Geneva, Switzerland, Mar. 2021.
[42] E. Andrukiewicz et al., *Methodology for Sectoral Cybersecurity Assessments*, Eur. Union Agency Cybersecur. (ENISA), Attica, Greece, Sep. 2021. [Online]. Available: https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment
[43] *Security Assurance Specification (SCAS) for the Next Generation Node B (gNodeB) Network Product class*, Standard ETSI TS 133.511 V17.1.0, May 2022.

Jordi Mongay Batalla received the Ph.D. and D.Sc. degrees. He is currently an Associate Professor with the Warsaw University of Technology. He is also a CEI Expert of the European Union Agency for Cybersecurity (ENISA) for 5G Cybersecurity. He has coordinated more than ten research projects. He is an editor of four books and the author of more than 200 papers published in books and international journals. He is/has been a guest editor and a member of the editorial board in more than ten international journals. He is in the 2% higher researchers in 2021 (Elsevier list).

Luis J. de la Cruz Llopis received the Ph.D. degree in telecommunications engineering from Universitat Politècnica de Catalunya (UPC), Barcelona, Spain, in 1999. He is currently an Associate Professor with the Department of Network Engineering, UPC. He is also with the Smart Services for Information Systems and Communication Networks (SISCOM) Research Group, where he participates in research projects in collaboration with different European public universities and collaborates with private companies in the development of technological communications projects. His research interests include the application of machine learning techniques in wireless multi-hop and C-V2X networks and the development of IoT smart services.

Germán Peinado Gómez received the M.Sc., M.S.I.S.T.M., and Ph.D. degrees. He is currently with the Warsaw University of Technology. His research interests include 5G networks, roaming, cybersecurity, standardization, risk management, information security, and applied machine learning. He is also a Senior Security Solution Consultant with the Nokia Security Centre of Excellence, where the main responsibility resides on the definition and design of security blueprints and architectures for 5G networks. He possesses 20 years of experience in telecommunications industry, having been involved in multiple projects for carrier grade operator networks. He holds several recognized security certifications, including CISSP, CCSP, and CISM. He also holds an ISO/IEC 27001 Lead Auditor.

Elżbieta Andrukiewicz received the Ph.D. degree. She is currently an expert on information security management systems. Her research interests are methods for information and ICT security assessments and evaluations, information security management system development and implementation, methods, development and integration of the risk management systems in organizations, information, and ICT security audits. She is also a Standardization Expert of the ISO/IEC JTC1 Subcommittee Information Techniques—IT Security Techniques" and an editor of several international standards for information and ICT security. Working recently for ENISA and the European Commission. She is also the Project Manager of the Polish National Scheme for ICT Product Security Evaluation and Certification Compliant to Common Criteria.

Piotr Krawiec received the Ph.D. degree from the Warsaw University of Technology (WUT), Poland. He is currently an Assistant Professor with the Institute of Telecommunications, WUT. Since 2012, he has been with the National Institute of Telecommunications (NIT), where he has been the Technical Manager of Information Technology Security Evaluation Facility since 2020. He is also a cybersecurity laboratory accredited to conduct evaluations and validations according to the common criteria and ISO/IEC 19790 reference standards with NIT. His research interests focus on cybersecurity evaluation of network devices and services, IP technologies, and applications for the future internet.

Constandinos X. Mavromoustakis (Senior Member, IEEE) received the B.Sc., B.Eng., and M.Eng. degrees in electronic and computer engineering from the Technical University of Crete, Greece, the M.Sc. degree in telecommunications from the University College of London, U.K., and the Ph.D. degree from the Department of Informatics, Aristotle University of Thessaloniki, Greece. He is currently a Professor with the Department of Computer Science, University of Nicosia, Cyprus. He is also leading the Mobile Systems Laboratory, Department of Computer Science, University of Nicosia, with a dense research work outcome, whereas he has served as a consultant to many industrial bodies and participated in several projects.

Houbing Herbert Song (Fellow, IEEE) received the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, USA, in August 2012.

He is currently a Professor and the Director of the Security and Optimization for Networked Globe Laboratory (SONG Laboratory), University of Maryland, Baltimore County (UMBC). His research interests include the cyber-physical systems/Internet of Things, cybersecurity and privacy, and AI/machine learning/big data analytics. He is also an ACM Distinguished Member. He has been a Highly Cited Researcher identified by Clarivate (2021 and 2022). He received IEEE 2021 Harry Rowe Mimno Award and more than ten best paper awards from major international conferences.