



HAL
open science

Trustworthy AI for 5G: Telco Experience and Impact in the 5G ESSENCE

Maria Rita Spada, Alessandro Vincentini

► **To cite this version:**

Maria Rita Spada, Alessandro Vincentini. Trustworthy AI for 5G: Telco Experience and Impact in the 5G ESSENCE. 15th IFIP International Conference on Artificial Intelligence Applications and Innovations (AIAI), May 2019, Hersonissos, Greece. pp.103-110, 10.1007/978-3-030-19909-8_9 . hal-02363850

HAL Id: hal-02363850

<https://inria.hal.science/hal-02363850>

Submitted on 14 Nov 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

Trustworthy AI for 5G: Telco experience and impact in the 5G ESSENCE

Maria Rita Spada¹ and Alessandro Vincentini¹

¹ Wind Tre S.p.A, Largo Metropolitana 5, 20017, Rho (MI), Italy

www.windtre.it

Abstract. This paper discusses how it is possible to implement a general model to cope with the network and service management when the AI (Artificial Intelligence) capabilities are integrated in a trustworthy AI for 5G solutions framework. We discuss the general regulatory considerations related to the AI introduction in the 5G network management as this has been examined as part of the H2020 Project 5GESSENCE.

Keywords: 5G Networks, AI; Agents; BSS; Neutral Host; OSS; Trust

1 Introduction

The telecommunications are one of the most interesting contexts involved in the process of the AI (Artificial Intelligence) development, because in real life situations it might happen that sensors, actuators and AI agents are away from each other and one -or more- telecommunications network(s) lay in between and connect them.

In general, the communications networks are clearly the infrastructure that transfers the information generated by the sensors to the remote AI agents. The new 5G and FTTH (Fibre-to-the-Home) networks are the main connective tissue of the artificial intelligence systems located throughout the territory.

When a Telco operator wants to use the new solution based on AI, it is important to take into account some “values” with which AI should comply to set out several concrete requirements (such as privacy, accountability and transparency) for AI systems integrated with other systems used to create value and to deal with the complexity of the information and communication aspects.

Given the complexity of the services offered, it is necessary to use policies on different levels so that to evaluate AI models and their integration in the normal context. When a Telco includes AI solutions it is necessary to develop governance frameworks in order to make sure that AI development does not infringe upon different aspects, like human rights, freedoms, dignity and privacy; there will be the possibility of programming, by using the AI solutions, co-robot ethics to legal and other questions, including liability and privacy concerns. In this framework, the Telecom Operator must have a reliable approach on trustworthy AI so that to offer solutions that “people can trust”, according to transparency and responsibility requirements.

The present paper is organized as follows: Section 2 describes the new approach for realizing trustworthy AI for 5G solutions; Section 3 describes some AI applications in the network, with a particular focus upon the 5G network; an overview of the general architecture and how this can be deployed is introduced in Section 4, taking into account as reference the 5G ESSENCE solution. Section 5 underlines the benefit of the new approach and the improvement of the realization and management of the network slicing concept -or of other aspects- correlated when using the AI solution.

2 Approaches for Realizing Trustworthy AI for 5G Solutions

It is important to take into account the concept of the model for network management that can be implemented by using the 5G capabilities, when it is also possible to integrate the AI capabilities.

In fact, when we design the network slicing model for a Telco, or more generally for a Neutral Host, an intermediate provider between manufacturer or RF equipment provider and Mobile Operators/Service Providers, we have to deal with the possible conflict in the network between special services and equally worthy of protection, such as that which is given to an electro-medical device or to a machine that can manage the braking system of a vehicle. Which of the two applications is more appropriate to give priority in case of problems? How is this decision made? To date, there is no clear answer; perhaps the only principle that can be considered is that it should be established *a priori* in order to define some rules that will be applied, when we have millions of people using such services. The first aspect to be defined is that of the relationship(s) between the network operators, the software and hardware developers, the deployers and the customer(s). Everyone among these has a central but different role, and everyone has different responsibilities.

The network indeed can experience congestion or outages and, when this occurs, the transferred information can be delayed or even discarded. Networks, in fact, are dimensioned when using the criteria adopted to define the slices.

From a Telco's point of view, two important safety properties must be guaranteed and these have already been explored by the researchers, that is: the "safe *interruptibility*" and the "*distributional shift*", where:

1. Safe interruptibility is the ability to interrupt an intelligent agent and override its actions at any time.
2. Distributional shift is the ability of the AI system to behave robustly when the environment where it operates differs from the training environment.

According to this vision, a Telco is not responsible for any failure not being able to achieve the two properties, as mentioned above. The reason why networks cannot be considered as responsible of the possible fallacies of the ensemble "sensors-actuators-AI agent" is that zeroing the probability of congestion would require infinite network resources, which is clearly impossible. A fall-back strategy for the AI agent in this scenario is in charge to developers, expected "by design": it is important to create a strong ecosystem to share this approach. The AI equipment should sense the "hiccup

information” of the surrounding congested networks and swiftly stop what it is doing, thus applying the principle of safe interruptibility.

This applies even more when the consequences of wrong decisions made by an AI used are well diverse, depending on the field these are made. Wrong decisions in a medical context are clearly much worse than a wrong suggestion provided to a consumer by a recommender system. It is important to share common guidelines to cope with these aspects; besides it should be requested to have clear and unequivocal criteria to support an electronic communications network operator so that to make choices when network resources are insufficient to manage one or more mission critical services that transit networks simultaneously.

In the event an inconvenience is unavoidable anyway, e.g. when humans are damaged, injured or killed due to a decision taken by AI systems, AI system must decide with fairness.

Another issue, important from a Telco’s point of view, is the correct assessment of the security measures to be provided for AI systems when we include this in the operational context integrating the new features in the different systems. In particular, it might be useful to define a classification of AI systems according to their intended use in order to define the security measures adequate to the context of applications, as discussed in “Ethics guidelines for the development and use of artificial intelligence” **Errore. L'origine riferimento non è stata trovata.**

It is also important to define security measures to ensure the availability and integrity of data throughout the life cycle of the entire AI system. Among the measures that help to ensure the robustness of the AI system is necessary to foresee the segregation of all environments, including those provided for the AI training.

According to Telco’s experience, the human supervision is only one of the possible instances of governance of all these elements; with more experience, it could be possible to evaluate the hypothesis of the aid of other AI systems to support human supervision, which carry out extemporaneous (therefore unpredictable) redundancy checks in environments separated by AI system to be governed in a sort of “logic” of “assisted governance”. The autonomy of the AI system also depends on its ability to interact: that is, some context in the network management could be used as first field for the application of this approach.

This concept of governance then extends to the autonomous interaction of the AI system with other systems networks and devices; in this way it could be possible in the near future that network systems could be equipped with the capacity to autonomously expand their interactions within a predefined “evolutionary perimeter” during the design phase.

The AI, equipped with its own start-up of a minimum set of connections to protect potential vulnerabilities, could independently activate further systemic interactions to increase its evolutionary degree. The improvement in efficiency would correspond to a reduction in risks related to vulnerability. This will improve the capacity to include the AI in the Telco’s context to manage better the network and the final services to the end-users.

In particular, we believe that an assessment lists should be enriched by items to detect the correct application of “*safe interruptibility*” and “*distributional shift*”, or other applicable procedures to avoid danger in case of outage of communication networks.

Further fine tuning should be applied on supervised machine learning algorithms and AI's essentially learn what they are taught. Therefore, for them to be fair and non-discriminatory, a proper choice of the training set is crucial to avoid imbalances and inequalities when classifying (i.e. with the term "imbalance" we mean that the classification results are not distributed evenly across all the classes forming the domain of the classification problem).

Since miss-classification might lead to uneven decisions and bias reinforcement, an approach to mitigate the risk of miss-classification could consist in the assessment of the training sets in search of imbalances not necessarily intended.

Moreover, we generally agree on the principle that it is needed to guarantee not only the concept of "privacy by design" but also the concept of "ethics by design"; in this way, we require ethical principles (and privacy) to be embedded in AI products and/or services, right at the beginning of the design process.

In fact, ethics must be embedded into the design and development process from the very beginning of the AI creation and those ethics must be aligned with the values and ethical principles of a society or of the community it affects. For this reason, it could be necessary to use the same approach in Europe to guarantee the process. Each company has to share a common vision and follow an internal procedure to guarantee principles for trust and transparency. By adopting and practicing this approach, it could be more clear and transparent about how to use the AI solutions in different contexts.

3 AI packed Approach to 5G Business Case

Artificial Intelligence requires an ongoing and interdisciplinary effort to cover all the effects in the different ecosystems where the new approach will be introduced. Guidelines should give clear and unequivocal criteria to support a communications network operator so that to make choices when network resources are insufficient in order to manage one or more mission critical services that transit networks, simultaneously: the consequences of wrong decisions made by an AI are well diverse depending on the field they are made. Wrong decisions, in a medical and/or transport contexts, are clearly much worse than others. Therefore, we think that the regulation of the safety topic should be domain specific.

In the same way, it is important to realise "Trustworthy AI" according to a shared framework compatible with the general architecture described in [2]. We look at the opportunities of enhancing our tools for the management of the network and to improve our OSS (Operations Support Systems) services -or in other sectors- so that AI can be "trained" to help improve diagnoses -or other outcomes- to improve the quality of the final services in different contexts (such as smart mobility, smart cities or industry 4.0).

The OSS/BSS (Operational and Business Support Systems) service provides Operating and Business supports functions in order to manage the network infrastructure (OSS) as well products, customers and customer life cycle (i.e.: Orders, Upgrades, Complains, Usage & Invoicing, Leave) of the services provided by the operators (BSS).

The need for highly automated processes is particularly stressed from a telco's point of view, due to frequency/network/IT (Information Technology) resource sharing in deployment and provisioning processes, having in mind the maximisation of the customer experience, services and network resources.

As the network infrastructure moves towards virtualized infrastructures, OSS and BSS systems evolve the virtualization path based on IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service) or SaaS (Software-as-a-Service), by using a common commercial hardware and storage and by providing separate virtualized infrastructure, virtualized platform and virtualized software to a set of tenants using the shared physical infrastructure. Specific application environments can be then made available for vertical implementations, including Artificial Intelligence and Machine Learning functionalities in order to provide enhanced analytics needed for a quick service time to market. In the following we discuss a few examples of telco's contexts in which we think that the introduction of AI will be an important challenge to improve the Telco's role:

1. **Network Management:** More and more data are generated by devices across the network and used to manage itself; other network sources can provide insight into how networks are performing. The way how that data is collected and analyzed to provide meaningful and actionable information is the "key" to make a difference in network operations. The AI tools can help Telcos to monitor and evaluate network performance and these tools are comprehensive enough to deliver a complete and holistic picture of the entire network (from the user terminal to the cloud through the edge).
2. **Product Management:** A Telco organization is typically responsible for managing the Product/Service Catalogue through the assembly and update of products utilizing available components. The definition of a "product" is an item that satisfies a market's want or need. The introduction of the AI approach will improve the Telco's ability to create and maintain products that can be sold to customers in the target market. It could be possible via using the AI approach to model the structure of a product, creating and managing this in a "catalog" of products or a number of components associated together to create new opportunities to reduce the time to market. According to this, some of the components within a product will be enabled by shared/common/reusable resources (e.g., network exchange) that may be managed by different parts of the organization, improving the global efficiency of a Telco organization.
3. **Customer Contact Management:** Another context in which the introduction of an AI approach is important, is the "customer contact management" dealing with the retention and loyalty aspects; the Customer Relationship Management (CRM) suite allows a telco operator to create, update and view the customer's information (i.e.: names, addresses, phone numbers, organizational hierarchy), as well as to record and view all customer interactions across different communication channels and department. The AI solution will offer better capabilities to highlight customers as risk of switching to an alternative carrier and provide comparisons with other operator's service packages, allowing customer care agents to provide advantages for the business intelligence platforms.
4. **Customer Order Management:** Starting from the telecoms experience, the introduction of AI solutions will help in the design, price and the lifecycle of the

proposed services. Besides, the AI will offer support to negotiation and closure of a formal contract with the customers to deal with the creation of the customer's contract and of any associated service level agreements, including approval of custom language, customer contract sign-off, appropriate counter signature and contract expiration taking into account all the "smart" elements coming from an analysis based upon AI tools. In particular, Customer Order Management application handles order requests to suspend, resume, change ownership, amend, add, change and discontinue existing ordered products. By using AI it will be easier to deal with repackaging of the purchased offers into alternate product offering (may require sales/contract negotiation).

In the telco contexts in which we think that the introduction of AI will be an important challenge to improve the Telco's role, as discussed, the AI is going to be part of any application and network controller. In 5G scenarios we can assume that AI solutions can be part of business proposition of specific use case. In particular, proposition depends upon specific use case; when assuming a Network Slice for a Smart City scenario the proposition could include specific AI services for sensor to be deployed on edge or in the scenario of broadband network slice AI-based monitoring within vEPC (virtualised Evolved Packet Core) solution.

4 The 5G ESSENCE Solution

The 5G ESSENCE project **Errore. L'origine riferimento non è stata trovata.** addresses the paradigms of Edge Cloud computing and Small Cell as-a-Service (SCaaS) by fueling the drivers and removing the barriers in the Small Cell (SC) market, forecasted to grow at an impressive pace up to 2020 and beyond and to play a "key role" in the 5G ecosystem. The project defines the baseline system architecture and interfaces for the provisioning of a cloud-integrated multi-tenant Small Cell network and a programmable radio resources management (RRM) controller.

The introduction of AI solutions will improve the capability of the system to development of the centralized software-defined radio access network (SD-RAN) controller to program the radio resources usage in a unified way for all CESC (Cloud-Enabled Small Cells) and to distribute service management in a multi-tier architecture.

As already introduced, the 5G ESSENCE offers an innovative architecture, capable of providing Small Cell coverage to multiple operators "As-a-Service", enriched with a two-tier architecture: a first distributed tier for providing low latency services and a second centralized tier for providing high processing power for compute-intensive network applications. To that end, 5G ESSENCE envisages to virtualize and to partition Small Cell capacity while, *at the same time*, it aims to support enhanced edge cloud services by enriching the network infrastructure with an edge cloud.

The introduction of the approach based on AI techniques in a project like the 5G ESSENCE will improve the capabilities of the solution not only to cope with the complex network based on the combination of MEC (Mobile Edge Computing) and NFV (Network Function Virtualisation) concepts with Small Cell virtualization in 5G

networks, but also to cope better with the complex ecosystem required for supporting multi-tenancy and for increasing the network capacity and the available computational resources at the edge.

The proposed solution allows multiple network operators (tenants) to provide services to their users through a set of Cloud Enabled Small Cells deployed, owned and managed by a third party (i.e., the CESC provider). Fig. 1 shows a high level view of the envisaged architecture.

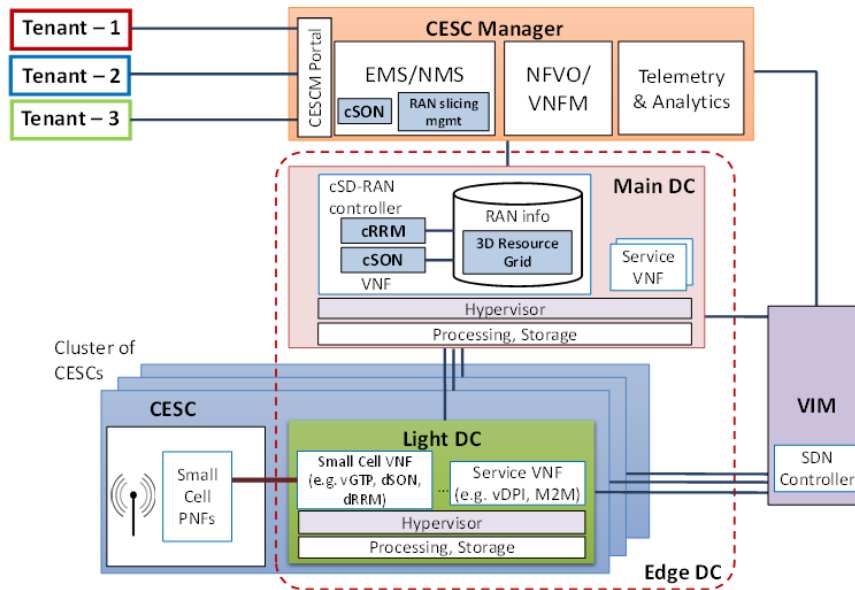


Fig. 1. 5G ESSENCE architecture

In the 5G ESSENCE architecture **Errore. L'origine riferimento non è stata trovata.** the NFVI (Network Function Virtualization Infrastructure) spans across the Main Data Centre-DC (i.e., the core cloud) and Light DCs (i.e., edge clouds), and this requires dealing with wide distribution and heterogeneity. The high dynamicity characterizing the system calls for an efficient, distributed and adaptable monitoring system. The monitoring data is provided to an analytics engine to extract insights for the support of orchestration decisions and to enable efficient resource allocation across the overall infrastructure. An end-to-end orchestration of infrastructure and services is crucial for reliable deployment and execution of services. The 5G ESSENCE orchestration platform also manages the lifecycle of services and it fully supports an ETSI-based view of the MANO (MANagement and Orchestration) [5]. For all these reasons this context could be a good reference point to start in the evaluation of the AI introduction, to improve the global systems using an approach like the Machine Learning as a Service (MLaaS) or the ML Market Places; it could be possible to install specific algorithm at edge level or in the distributed sensors or to use specific APIs, as suggested by some already available solutions described in [6] or in [7].

5 Conclusion

The integration of such AI capabilities demonstrates how the new integrated approach contributes to 5G architectural concepts such as, for example, the improvement of the realization and management of the network slicing concept or the other aspects correlated to the BSS/OSS context, in particular enriching the 5G services catalogues with different AI-based functions.

Acknowledgements. This work has been partly funded by the EC in the context of the 5G ESSENCE project (Grant Agreement No.761592).

References

1. Ethics Guidelines for the development and use of artificial intelligence (AI), https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_draft_ethics_guidelines_18_december.pdf, December 2018
2. 5G-PPP-5G-Architecture-White-Paper-Jan-2018-v2.0
3. Embedded Network Services for 5G Experiences” (5G ESSENCE) Project, Grant Agreement No.761592, DoW
4. 5G ESSENCE Project, “D2.2: Overall System Architecture and Specifications“, 5G ESSENCE WP2, February 2018
5. ETSI, “Network Functions Virtualisation (NFV); Management and Orchestration 001 V1.1.1,” December 2014. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/nfv-man/001_099/001/01.01.01_60/gs_nfv-man001v010101p.pdf
6. <https://cloud.google.com/products/machine-learning/?hl=it>
7. <https://azure.microsoft.com/en-us/resources/videos/an-overview-of-the-azure-machine-learning-marketplace/>