ETSI White Paper No. #34

Artificial Intelligence and future directions for ETSI

1st edition – June 2020

ISBN No. 979-10-92620-30-1

Authors:

Lindsay Frost (Document editor, NEC)

Tayeb Ben Meriem (ORANGE)

Jorge Manuel Bonifacio (PT Portugal)

Scott Cadzow (Cadzow Consulting)

Francisco da Silva (Huawei)

Mostafa Essa (Vodafone)

Ray Forbes (Huawei)

Pierpaolo Marchese (Telecom Italia)

Marie-Paule Odini (HPE)

Nurit Sprecher (Nokia)

Christian Toche (Huawei)

Suno Wood (eG4U)

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org

Contents

Executive Summary

This White Paper explores key issues of Artificial Intelligence (AI) that present both huge opportunities and new challenges for information and communication technologies (ICT). AI is becoming central to ETSI's mission of "being at the heart of digital". Standardization is understood to be a necessary tool in the efficient exploitation of these opportunities, both in Europe and globally.

This White Paper details current initiatives and recommends future directions for the ETSI community and the ICT industry in general. ETSI technical bodies are already addressing numerous aspects of using AI in ICT systems. These include 5G systems, network planning and optimization, service provisioning and assurance, operator experience, security, IoT, data management and testing. eHealth and Human Factors technical bodies are considering the use cases for AI and their potential impact on people.

This White Paper also discusses some activities of advisory groups, government-sponsored research projects, open-source AI projects, industry alliances and some SDOs, which are creating specifications. These groups are highly relevant as potential partners of ETSI in realizing the benefits of AI. This document recommends extending ETSI outreach activities towards them.

This White Paper makes several recommendations, including:

- continuous monitoring of AI activities in ETSI
- evaluation of the technical impact of EU ethical guidelines (See "Ethics Guidelines for Trustworthy AI". Published 8th April 2019 [1])
- continuing the effort to achieve interoperability
- supporting a strong focus on testing methods for systems that use AI
- evaluating the required quality of datasets, which may ultimately co-determine AI system performance.

Special Foreword: AI and Covid-19

This White Paper was drafted during the Covid-19 crisis, by a group of ETSI members, working online, as the world confined one quarter of its population to self-isolation at home. Governments have relied on fast ICT and quick analysis of data to aid decision-making while imposing this socially and economically devastating rule.

This confused and distressing environment has encouraged many people to consider in a positive light the future role of AI in the handling of medical and societal information. Government decisions have been seen to depend on the quality of information available and, at present, data and its modelling and processing is barely adequate to the enormous task of coping with the pandemic. The quality and timeliness of advice must be improved and Big Data, AI and ICT clearly have a significant role to play. The energy and drive to develop AI has already been boosted by the current crisis. It is likely to continue to grow as the world faces great challenges in data management and care of its citizens.

As is demonstrated in this White Paper, standardization by ETSI and other SDOs has a major role to play in future deployments of AI. The global trend now forming seeks to establish AI for the future benefit of all, observing the fundamental, ethical values as expressed by the European Union and other international, governmental and non-governmental organizations.

1 Introduction

Design and implementation of Artificial Intelligence is developing rapidly in many sectors of the global market. ETSI is the main European Standards Organisation charged with development of specifications for ICT systems, and how those systems work and interact is increasingly being impacted by Artificial Intelligence.

ETSI specifications as well as workshops, webinars and guides can offer practical support to the introduction of AI into many areas. Moreover, the implementation of AI will inevitably entail extensive and costly training/ educational programmes (for people), particularly given the uneven efficacy of current IT and knowledge management systems. Additionally, the use of AI is already arousing ethical considerations (see "AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense" [2]) that must be addressed and also be seen to be addressed since public fears of AI are not necessarily based on actual threats, but rather on a perception of loss of control.

This White Paper has three purposes:

1. to summarize aspects of AI that are currently used within ETSI Technical Bodies (TBs)
2. to examine the industry and standardization landscape
3. to highlight potential directions of AI strategic development in the ETSI community

This document considers AI as a means to derive insights automatically from data, based on an evolving set of statistical learning methods. Learning is the method used by the AI system to extract knowledge from the training data. An AI system that is trained and has learning in a particular field (such as image recognition, eHealth, networking and resource management, IoT, robotics, etc.) may continue to adapt with further online learning. It may also be given offline learning to refresh its awareness (re-training) of the situation. The resultant activity is only as good as the quality of the training of the AI system.

Many areas related to networks can benefit from AI, such as in the emerging paradigm of Autonomic Networks (also known as Self-Adaptive Networks or Smart Networks or Autonomous Networks in the literature). This benefit for networks can be understood (see ETSI GR ENI 007 v1.1.1 [3] for details) in terms of AI applicability to various problems in Autonomic (closed-loop) Management and Control (AMC) of networks and services, in producing:

- Assistance to humans: knowledge of network status, summarized for a human expert
- Partially automated networks: key performance indicators (KPIs) for hierarchical decision support are provided, together with appropriate actions for the human to approve/disapprove
- Fully automated response: ultimately taking action in case of a fully automated process chain (e.g. executing configuration changes to the Network and/or to improve business value).

The use of AI in ICT is considered to be a game changer, because it enables new business cases that take ICT beyond pure connectivity, supporting new services with added value and efficient operation. In the current crisis period of a health pandemic, ICT enhanced with AI can provide robust and sustainable logistics, as well as connectivity to citizens, and support to the health care sector (medicine development, medical knowledge sharing and disease spread monitoring, personal-distancing monitoring).

However, risks have been identified for AI applications, for example concerning the acceleration of possibly inappropriate responses, concerning incorrect modelling or insufficient training data, concerning

aspects of AI trust and explainability, and appropriate testing. Standardization can help to reduce such risks, for example by establishing standards for comparative benchmarking, for certifying models, for validating model integrity, etc.

2 Importance of AI Issues across Europe and Globally

The G20 meeting in June 2019 concluded with the 'G20 Ministerial Statement on Trade and Digital Economy' [4] containing a special section on AI and an Annex of principles for AI.

The EU is investing heavily in AI research and development as shown in the EU "Coordinated Plan on Artificial Intelligence" of December 2018 [5] and in the EU communication on Artificial Intelligence for Europe [6], including billions of Euros allocated in the "Digital Europe Programme" [7]. This is due to potential economic gains (e.g. see OECD reports on AI investments [8] and on AI patents [9]), as well as economic risks (such as the issue of liability – "Liability for Artificial Intelligence and other emerging digital technologies." [10]) and to avoid potential loss of leadership due to failure to act.

The EU has launched a 'human-centric' approach to AI, respectful of European values and principles, with a number of milestones shown below:

- In June 2018 the EU Council endorsed an ambitious Europe-wide Coordinated AI Action Plan [5], where standardization plays a role to support interoperability and exchange of data sets
- The March 2019 version of the European Commission (EC) Rolling Plan for ICT Standardisation [11] fostered coordination between SDOs on AI, since many of them are already engaged on AI.
- In April 2019 the EC HLEG (High Level Ethics Group) released a set of "Ethics Guidelines for trustworthy AI" [1]. The outcomes of the HLEG on AI included seven requirement categories (accountability, human agency, technical robustness, privacy and data governance, transparency, non-discrimination, and societal well-being) that the EC encourages to be considered in the EU standardization roadmap.
- In April 2019 a European Parliament study(see "A governance framework for algorithmic accountability and transparency" [12]) recommended the creation of a regulatory body for algorithmic decision-making, tasked with defining criteria that can be used to differentiate acceptable algorithmic decision-making systems.
- In July 2019 the EU adopted the new Regulation (EU) 2019/1150 [13] requiring providers of online intermediation services and online search engines to implement a set of measures to ensure transparency. The Commission is also carrying out an in-depth analysis on algorithmic transparency.
- In February 2020 the EC AI White Paper On Artificial Intelligence – "A European approach to excellence and trust" [14] acknowledged the need for a measured assessment of risk for the individual and for society at large. It supported traditional European values and fundamental rights, including safety and liability, and elimination of racial or gender bias. It recognised the need to build bridges between disciplines that currently work separately. The White Paper asserts that the EU is 'committed to enabling scientific breakthrough'.

The health sector offers the possibility of a rapid increase in useful big data sources in an environment challenged by overcrowding and strained resources. This provides a powerful impetus for the introduction of new AI services. This may often require more effective and efficient IoT systems to be in place prior to the design and implementation of the AI platform(s).

A key issue for ETSI and other standardization bodies is that the EC HLEG Guidelines for a trustworthy AI [1], and related guidelines, are differently from "usual" technical standards in that they are – by nature – difficult to encode in specifications, implement in solutions or verify in practice. This could become a burden especially for SMEs, and especially when compliance to those criteria becomes part of the requirements in public/private procurement.

3 AI in ETSI Standardization Today

AI is accelerating the digital transformation and ETSI is at the heart of digital. ETSI develops globally recognized ICT standards with direct impacts on Industry, SMEs, Academia, Citizens, and Public Institutions. The ETSI community has a strong interest in AI as a "tool": in architectural models, to enhance Information/data models, to redesign operational processes, to increase solution interoperability, and for data management for new ICT standards.

ETSI has been working with AI technology for some time, initially for optimization of complex networks and networks-of-networks. The special impact of non-deterministic aspects of AI on test scenarios (including the pre-test offline training of AI systems) is of growing importance, also for network conformance testing. With the growth of interaction between systems using AI, interoperability is a critical issue. Finally, the impact of AI on our lives, mediated by ICT systems, is set to be so large that the issues of ethics and liability must be covered. Standardization can provide technical specifications in response to political guidelines that can then be referenced in regulations, facilitating practical results.

A number of milestones in ETSI activities with AI are mentioned below.

In September 2017, ETSI presented at the Global Standards Collaboration meeting GSC-21 in Vienna its perspective on AI issues and an overview of related work in ETSI [15].

In March 2019, an ETSI presentation to the GSC-22 [16] included a set of key drivers of an ETSI roadmap on AI:

- Better education and awareness – among ETSI stakeholders and within the wide ETSI Community
- Impact analysis – ETSI TBs need to analyse possible impact of AI for their scope of work, including information models
- A novel ETSI technology roadmap on AI - new areas, elaboration of best practices, E2E approach
- An action plan - in line with EC AI Implementation Plans
- Increased Collaborations and Liaisons – with all the concerned SDOs

In April 2019, an ETSI Open Workshop on AI [17] suggested directions to improve the SDOs (and ETSI) footprint on the subject of AI and identified needs for standards:

- to ensure interoperability, harmonized terminology, concepts and semantics
- on horizontal levels over vertical markets
- for interchange formats for machine learning (ML) data models and algorithms interchange
- that ensure adaptive, agile governance of the system and foster piloting/testing
- providing a trustworthy AI framework for a "certification of AI"

The next sections provide highlights, grouped thematically, of current ETSI activities relate to AI.

3.1 AI in 5G Systems

ETSI is engaged in many activities regarding 5G. At the radio and mobile system level, the main specification work is developed by ETSI within 3GPP; whereas other activities falling under the 5G umbrella take place elsewhere in ETSI.

The overall trend with 5G expectations at the macro level is for a unifying connectivity platform for many applications, including those enabled by AI.

In 3GPP 5G specifications, AI is broadly referenced in the two main areas of Core Network capabilities (5G NG Core) and Radio Access Network (5G RAN). In both areas, AI plays the role of an ancillary layer that can increase 5G network automation and effective management and orchestration. This layer can provide, too, an augmented user experience by expanding the 5G device capabilities using cloud-based AI functionality.

AI has become an additional function in the management of RAN and the evolution towards the model of a SON (Self Organizing Network). In this field, ML (Machine Learning) can provide radio systems with the ability to automatically learn and improve from experience, without being explicitly programmed. This could become beneficial in radio contexts such as selecting the optimal 5G beam(s) and power level(s) configuration of a 5G cell at each transmission interval. Training of ML-based models can be based on the standardized collection of network configurations data together with corresponding network performances and traffic distribution, in order to predict network behaviour. Once trained, ML-based models could be deployed in the RAN to obtain optimal antenna and radio resource configurations.

In the 5G Core Service Based Architecture (SBA), the role of AI engines can be envisaged in the Network Data Analytics Function (NWDAF (see ETSI TS 129 520 V15.0.0) [18]), which provides the various Network Functions in the architecture with monitoring capabilities for the network or for the behaviour of specific customers. The 3GPP standard does not specify the architectural model of an AI solution in NWDAF, but just the service capabilities that are exposed and the way other 5G Core Network Functions can access the results.

3.2 Network Optimization and End-to-End Service Assurance

The pivotal deployment of 5G and network slicing has triggered the urgent need for a radical change in the way networks and services are managed and orchestrated. The ultimate automation target is to create largely autonomous networks that will be driven by high-level policies; these networks will be capable of self-configuration, self-monitoring, self-healing and self-optimization without further human intervention.

Machine Learning and in general Artificial Intelligence are key enablers for increasing automation. To deliver their full potential, AI-powered mechanisms require fast access to data, abstraction of intelligent and contextual information from events and rule-based systems, supervision, streamlined workflows and lifecycle management. Data includes known events in the near future and past cycles of usage (daily, weekly, monthly, annual, etc.).

Data is gathered from many sources:

(1) data from network functional elements;

(2) data from infrastructure (including cloud);

(3) data from user equipment;

(4) data from management systems;

(5) data from external systems (databases, applications, etc.).

It is possible that AI may be localized, may be used co-operatively across the communications network, or be within the individual services (e.g. eHealth, eTransport, etc.).

Network optimization with the aid of AI can operate at different time scales and may have a broader scope that includes intelligent management and control of resources and parameters of a network and of particular services. Examples of such network and service management and control intelligence are: Autonomic (i.e. Closed-Loop) Configuration management; Autonomic Fault-management; Autonomic Performance management; Autonomic Security management; Autonomic Monitoring management; etc.

Within ISG NFV (Network Function Virtualization), AI is being considered as a tool that eventually becomes part of the Management and Orchestration (MANO) stack. NFV virtualization is not explicitly considering AI, except in requirements to properly feed data and collect actions from AI modules [wi 1]:

> "Although NFV-MANO has already been equipped with fundamental automation mechanisms (e.g., policy management), it is still necessary to study feasible improvements on the existing NFV-MANO functionality with respect to automation [...] to investigate the feasibility on whether those automation mechanisms can be adapted to NFV-MANO during the NFV evolution to cloud-native."

ISG ZSM (ISG Zero-touch Network and Service Management), was formed with the goal to introduce a new end-to-end architecture and related solutions that will enable automation at scale and at the required minimal total cost of ownership (TCO), as well as to foster a larger utilization of AI technologies. The ZSM end-to-end architecture framework (see ETSI GS ZSM 002 [19]) has been designed for closed-loop automation and optimized for data-driven machine learning and AI algorithms. The architecture is modular, flexible, scalable, extensible and service-based. It supports open interfaces as well as model-

driven service and resource abstraction. Closed loops (e.g. using the OODA model of Observe, Orient, Decide, Act) enable automation of management tasks and allow e.g. continuous self-optimization, improvement of network and resource utilization, and automated service assurance and fulfilment.

The ISG ZSM is currently working to specify the closed-loop automation enablers, including automatic deployment and configuration of closed loops, means for interaction between closed loops (for coordination, delegation and escalation), use of policies, rules, intents and/or other forms of inputs to steer their behaviour, etc. In addition, the ISG is working to specify closed-loop solutions for particular end-to-end service and network automation use cases, based on the generic enablers and ZSM architectural elements for closed loops as defined in ETSI GS ZSM 002 [19].

The ETSI group ISG ENI designs “Experiential Networked Intelligence” based on data collection and processing using closed loop decision-making. The specification ETSI GS ENI 001 [20] demonstrates a number of use cases on service assurance, fault management and self-healing, resource configuration, performance configuration, energy optimization, security and mobility management. The specification ETSI GS ENI 005 [21] shows as a functional architecture how the data is collected, normalised and recursively processed to extract knowledge and wisdom from it. This data is used for decision-making and the results are returned to the network, where the behaviour is continually monitored. The requirements document ETSI GR ENI 007 [3] on network classification of AI details the use of AI in a network into six stages, from "No AI" to "full AI" deployment. Clearly, no network is at either extreme of the six stages.

ISG ENI is specifying training methods in document ETSI GS ENI 005 version 2 [21]. Training is often made with big data. Learning is the method used by the AI system to extract knowledge from the training data. Learning can take many forms: dictionary learning, rule-based learning, federated learning, supervised learning, reinforcement learning and “pure machine” unsupervised learning, or combinations of these. Training can be centralised, federated, umbrella-like or distributed peer-to-peer. An AI system that is trained and has learning in a particular field (e.g. image recognition, eHealth, networking and resource management, IoT, robotics, etc.) may continually adapt with further online learning, or may have offline learning to refresh its awareness of the situation (re-training).

TC INT Core Network and Interoperability Testing group created TS 103.195-2 for the Generic Autonomic Network Architecture (GANA) [22] and TS 103 194 “Scenarios, Autonomic Use Cases and Requirements for Autonomic/Self-Managing Future Internet” [23]. The optimization can be categorized as:

- Actions that are performed on network configuration parameters or network resources, e.g. transmission power, antenna tilt, routing policies, bandwidth allocation.
- Actions that are performed on the network structure, e.g. adding/removing network elements (either physical or virtualized instances). These actions imply configuration changes in order to accommodate the structural change.

TC INT specifications consider events that can trigger a network to dynamically change network properties. Events vary depending on the specific AI systems deployed in the network and the level where they operate, external or internal to the network. These events can occur in a chain-like fashion, e.g. policy change can trigger several secondary events in lower level functional units.

In conclusion, AI systems are already cited in many ETSI network specifications in ISG ZSM, NFV, ENI and TC INT, with an emphasis on dynamic optimization.

3.3 IoT, Data Acquisition & Management, Governance and Provenance

The impact of AI on data acquisition and management has already been considered in the above section, regarding network operations and network management. In this section, the aspects of AI related to application data will be considered, mainly for IoT-related standards.

SmartM2M has recently created two TRs to consider AI for IoT systems. The first of these, TR 103 674 Architecture AI4IoT [wi 2], addresses the introduction of AI/ML into IoT systems and the opportunities for improving AI/ML performance through use of the horizontal oneM2M standard and its family of common service functions (CSFs). The aim of the second TR, TR 103 675 PoCAI4IoT [wi 3], is to build and test a proof of concept that targets two technical innovations. One innovation involves extensions of existing CSFs to support new AI/ML-related functional requirements. The second innovation is to test the concept of new CSFs that offer AI/ML capabilities on an "as-a-service" basis. This could take the form of a configurable classification algorithm, for example, that one or more IoT solutions could access on a oneM2M-compliant IoT platform.

Another area in SmartM2M/oneM2M is the double role of AI in semantics:

- as a facilitator of the development and alignment of ontologies and semantics meanings, supporting human experts. This is in consideration as a further enhancement of the SAREF portal being finalized in 2020.
- for the provision of AI services to support IoT semantic interoperability, based on a common understanding of IoT information (both for people and machines) thanks to the SAREF family of ontologies, which support IoT information discovery, enrichment and validation.

The group ISG CIM (cross-cutting Context Information Management) considers exchange of data and metadata across systems to be crucial to input of information to AI platforms, to allow them to better filter information from “data lakes” and to create derivative information or decisions. ISG CIM so far considers provisioning of provenance, licensing information, data quality metadata, etc. as part of its NGSI-LD protocol (see NGSI-LD API, ETSI GS CIM 009 [24] and also security functions DGR/CIM-007-SEC [wi 4]). ISG CIM has not so far defined reference points specifically to higher-layer AI reasoning platforms. NGSI-LD API uses linked open data and property graphs to reference data definitions (ontologies) such as those in SAREF (See SAREF Smart Applications Reference Ontology. https://saref.etsi.org [25]).

The TC SmartBAN (Smart Body Area Network) reference architecture, defined in TS 103 327 [26], is managing semantic interoperability through an everything-as-a-service (XaaS) mechanism and a Web of Things (WoT) strategy. It should lead to the creation of new cross-domain applications in order to integrate SmartBANs into the Web of Things and more global scenarios. On the service and application side, generic service enablers and standardized APIs will provide secure interaction and access to SmartBAN data or entities (data transfer and sharing mechanisms included), embedded semantic analytics (device/edge/fog levels), automated alarm management, distributed monitoring or control operations. This offers a foundation to AI systems which might use the data, or be given secured access to control eHealth mechanisms. Such use cases are however not yet documented.

ISG ARF (Augmented Reality Framework) is defining an interoperability framework for augmented reality (DGS/ARF-003 [wi 5]) after thoroughly studying the existing SDO landscape in the report ETSI GR ARF 001 [27]. The AR Framework provides reference points for Interactive Contents and World Knowledge, which would allow external AI platforms to inject information/objects/actions into the augmented reality view. In such a case, the ARF platform would become a visualization tool for outputs of an AI system.

In conclusion: ETSI TC SmartM2M is considering the use of AI in IoT systems for semantic interoperability and for the development process of ontologies themselves, as well as addressing the opportunities for improving AI systems performance through the use of oneM2M. ISG CIM considers how to label and manage data to provision provenance and quality information as well as semantic interoperability (including to AI systems). TC SmartBAN considers interfaces which would allow semantic interoperability of eHealth sensors with external systems (including by default AI) and ISG ARF is defining a framework which would allow visualization of outputs of AI systems.

3.4 Security and Privacy

The rapid expansion of AI into new industries with new stakeholders, coupled with an evolving threat landscape and huge growth in AI, presents a number of tough challenges for security and privacy: assuring the provenance of the data, providing explainability of data processing, and avoiding misuse of AI systems for generating cyber-attacks.

As has been noted throughout this document, AI impacts our lives every day, from local AI systems on mobile phones suggesting the next word in our sentences, to large manufacturers using AI to improve industrial processes. AI has the potential to revolutionize our interactions with technology, improve our quality of life and enrich security – but at the same time, AI has the potential to create new attacks and worsen existing security measures.

ETSI ISG SAI (Industry Specification Group on Securing Artificial Intelligence), in close collaboration with ETSI TC CYBER, has undertaken to improve the security of AI through the production of standards to preserve and improve the security of new AI technologies.

The ISG SAI develops technical specifications and reports to address three aspects of AI in standards:

- securing AI from attack: where AI is a component in a system that needs protection,
- mitigating against malicious AI: for example where AI is used to enhance conventional attack vectors,
- using AI to enhance security measures.

The graphical representation in Figure 1 makes clear that there is a cyclical dependency of each of these elements. One of the roles of ISG SAI, and the work it will seed in TC CYBER and other groups, is to seek to minimize harm from AI and maximize benefit.

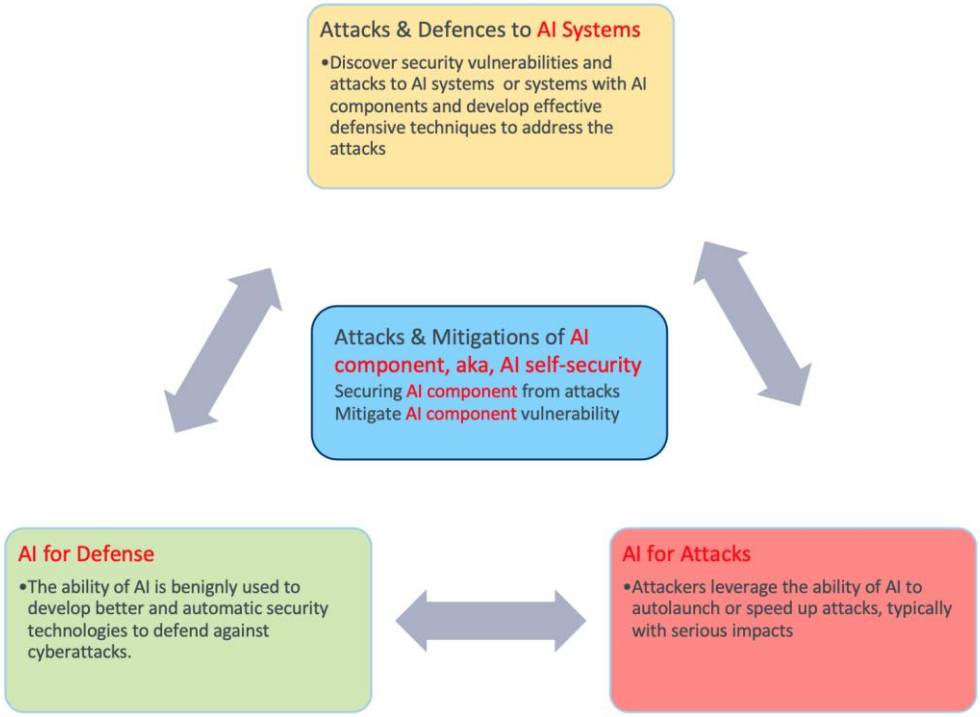

Figure 1: Interdependency of securing, enhancing and mitigating against attacks on/using AI (see ETSI ISG Securing Artificial Intelligence". Published 4th March 2020 [28])

The ISG SAI outputs will initially centre round the following five key topics and deliverables:

1. Problem Statement, that will guide the work of the group;
   DGR/SAI-004 [wi 6] will define and prioritize potential AI threats along with recommended topics for the ISG SAI to consider. The recommendations contained in this specification will be used to define the scope and timescales for the follow-up work.
2. Threat Ontology for AI, to align terminology;
   DGR/SAI-001 [wi 7] seeks to define AI threats and how they differ from threats to traditional systems. In doing so the AI Threat Ontology specification will attempt to provide a path to align terminology across different stakeholders and multiple industries, including adversarial AI attack analysis.
3. Data Supply Chain Report, focused on data issues and risks in training AI;
   DGR/SAI-002 [wi 8] considers that data is a critical component in the development of AI systems and access to suitable data is often limited, or even has been compromised so as to be a viable attack vector against an AI system. This report will summarize the methods currently used to source data for training AI, review existing initiatives for developing data sharing protocols and analyse requirements for standards for ensuring integrity/confidentiality in the shared information.
4. Mitigation Strategy Report, with guidance to mitigate the impact of AI threats;
   DGR/SAI-005 [wi 9] summarizes and analyzes existing and potential mitigation against threats for AI-based systems and produce guidelines for mitigating against threats introduced by adopting AI into systems.

5. Security testing of AI specification, in DGS/SAI-003 [wi 10], will identify methods and techniques for security testing of AI-based components, and produce a thorough gap analysis to identify the limitations and capabilities in security testing of AI.

In addition to the new work of ISG SAI, the ISG ZSM conducts security studies within its scope to identify security threats and motivate new standards. Security aspects are essential to address because the threat surface is extensive in the ZSM environment, due to the openness of the ZSM framework and the nature of emerging technologies such as AI/ML. In addition, compliance with country/region/industry security laws and regulations, including those related to AI, is and will be an obligation for ZSM service providers and their suppliers.

To summarize, security and privacy issues require assuring the protection of users of the ICT systems that embed AI. ETSI has core competence in these areas.

3.5 Testing

TC MTS (Methods for Testing & Specification) provides a special service within the ETSI community, according to its charter, to be 'responsible for the identification and definition of advanced specification and testing methods, that take advantage of innovative techniques to improve the efficiency and economics of both the standard description and associated conformance and interoperability testing processes' ... including using AI.

TC INT has already proposed an AI Model Life Cycle Management Process in the ETSI GANA Model of the White Paper #4 on 5G Network Slicing PoC [29]. It covers Development, Training, Testing, Certification, and Deployment, with three main associated stakeholders: AI Regulator / Auditor, 3rd Party AI Model Tester, AI Model dependent Certifier. Each stakeholder is considered to provide a related support as a component of what is named as an AI Support System.

TC INT has identified in EG 203 341 [30] a need for a “Test & Certification Framework for AI Models for AMC” to support the Industry in implementing Multi-layer AI Frameworks. To fill this need, TC INT first published White Paper #5 [31] and launched an ETSI Work Item “AI in Test Systems and Testing AI Models” [wi 11] that covers the following topics in collaboration with TC MTS and the ETSI Centre for Testing and Interoperability (CTI):

1. A general guide on the benefits of AI in Test Systems, with illustrations of AI in Test Systems
2. A general guide for testing AI Models in general, and the definitions of standardized metrics for measurements and assessments in Testing and Certification of AI Models, including certification of AI models of Autonomic Components/Systems
3. Testing ETSI GANA Models Cognitive Decision Elements (DEs) as AI Models for Autonomic (Closed-Loop) Network Automation, in the space of Autonomic Management & Control (AMC) of Networks and Services, with illustrations of AI Models for Autonomic Management & Control of 5G Network Slices
4. Generic Test Framework for Testing ETSI GANA Multi-Layer Autonomics & their AI Algorithms for Closed-Loop Network Automation (EG 203 341 [30]).

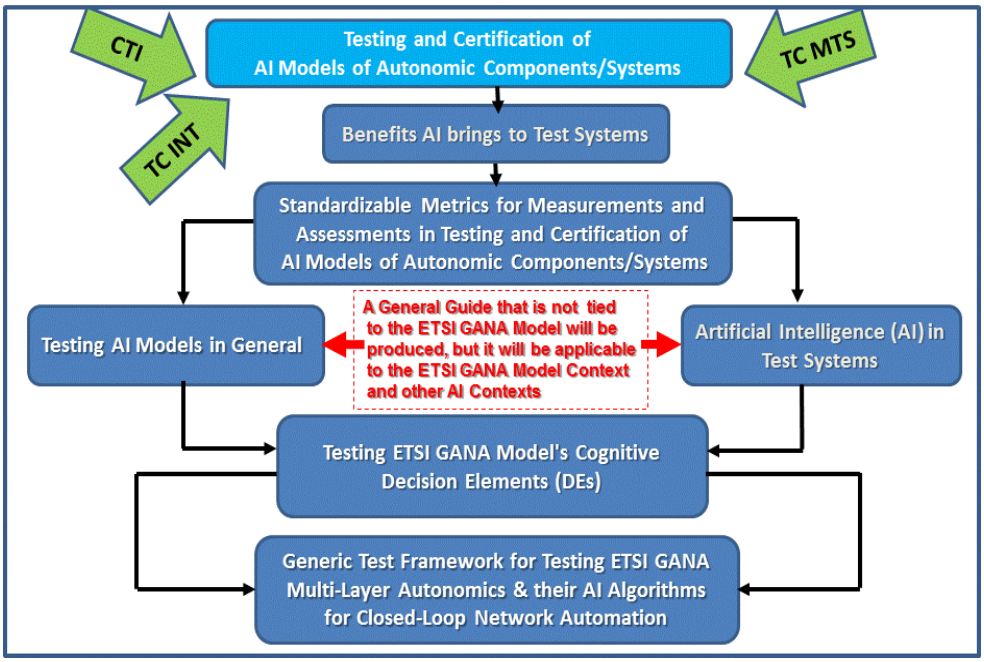

Figure 2: Deliverables planned for AI Testing by TC MTS, CTI and TC INT

The specifications address two challenges for Communication Service Providers (CSP):

- **Testing Offline AI Models** that need a programmable configurable (re)-training process in the CSPs' training environment before being exposed to new data (real data) in the production environment
- **Testing Online AI Models** that have the ability to learn and adapt their behaviour at runtime, when they are deployed in the CSP's production environment, continuously exposed to real and new data.

A Generic Test Framework for testing AI models/systems during their lifecycles needs to identify different types of test systems that could be employed to the problem space of testing AI Models: from those applied in phased testing starting at design time, up to those at the point when a network consisting of trusted and certified AI Models is tested as a whole (for integration and user acceptance testing).

There are various types and phases of testing and associated test systems and components that should be applied in testing AI Models, including the following: Conformance Testing, Interoperability Testing, Integration and User Acceptance Testing, Self-Testing. More details can be found in references ETSI DGR/SAI-004 [wi 6], WHITE PAPER #5: Artificial Intelligence (AI) in Test Systems, Testing AI Models and ETSI GANA Model's Cognitive Decision Elements (DEs) via a Generic Test Framework for Testing GANA Multi-Layer Autonomics & their AI Algorithms for Closed-Loop Network Automation [31] and ETSI Whitepaper #4: "ETSI GANA Multi-Layer Autonomics & their AI Algorithms for Closed-Loop Network Automation [32].

The European Commission White Paper of 19th February 2020 on Artificial Intelligence - A European approach to excellence and trust [14] mentioned many times the need for: a regulatory framework, creation of an AI testing centre and creation of a certification centre. There is a good mapping with the

aforementioned TC INT AI Model Life Cycle Management Framework. Therefore, this testing work in ETSI should be further aligned with the EC white paper and operationalize those three main recommendations.

3.6 Health and Societal Applications of AI

The EP eHealth group is actively discussing the role of AI in health, which offers opportunities to broaden diagnostic and treatment practice. However, access to appropriate data sources is a pre-requisite for such new applications. There is also an underlying requirement to have appropriate sensor and actuator systems (IoT) in place.

For AI systems to be deployed rapidly and usefully, society needs an assurance that people are protected from risk, both physical, and moral or ethical. There is public concern as to the safety and privacy/security of AI when used in the health domain. The EP eHealth group and others in ETSI are considering these issues. Since procurement and policy decisions for AI systems are often taken by non-technical experts, there is a need to make technical information appropriate and accessible. Standardization offers real support to this process by providing clear descriptions of AI systems, including for monitoring and control.

A firm foundation for the use of AI in health is being established with the successful introduction of robotic devices into everyday surgical procedures, such as appendectomy and knee replacement. Another example is the use of AI in pattern-recognition to assist in assessment of mammograms and prostate cancer scans. The role of AI in any diagnostic or treatment decision requires evaluation and comparison, with engagement of medical professionals who are trained under the traditional Hippocratic Oath (and its modern equivalents such as "Modern Hippocratic Oath holds the underlying values of medicine in a digital world" published 13th July 2018 [33]). It is clear that the role of ethics will dominate the environment for the design and usage of AI services for health in the same way that it has dominated medical services for millennia. This is further discussed in the recent EC White Paper on AI [13].

The group SC EMTEL (Special Committee on Emergency Communications) is currently updating two specifications related to IoT and AI. One specification describes requirements for communications from authorities/organizations to individuals, groups or the general public in emergency situatiions [wi 12] . The other specifies requirements for communication between authorities/organizations during emergencies, to accommodate communications involving First Responders and IoT devices [wi 13].

SC EMTEL is planning to investigate AI in the response to emergencies, not only for mission critical aspects, but also for accuracy and display of geo-location, including overlaying and combining different media.

3.7 Summary

Based on all the above, a matrix of current AI work areas within the ETSI community can be drafted, in a phased hierarchy starting with the conceptual terminology and ending with practical KPIs. Each group in ETSI may have a different set of needs and hence a different approach. For example, TC ITS has noted that it is not defining AI implementation solutions as such, but rather focuses on protocols and management of data which is used by (proprietary) AI entities. The mapping shown in Table 1 below is preliminary.

Table 1: Initial Mapping of AI Standardization Activities within ETSI

= considering = started = strong	3GPP	EP eHEALTH	ISG ARF	ISG CIM	ISG ENI	ISG MEC	ISG NFV	ISG SAI	ISG ZSM	oneM2M	SC EMTEL	TC CYBER	TC INT AFI WG	TC SmartM2M	TC MTS
Terminology					◕			◕	◕	◔			◕	◔	◕
Use cases	◔	◔			◕	◑	◑	◑	◕	◔	◔		◕	◔	◕
Impact of EU ethics guidelines		◕						◑		◔				◔	◔
Trustworthiness & Explainability		◑						◑	◔	◔				◑	◔
Security/privacy		◕		◔	◔			◑	◕	◔		◕	◔	◔	◔
Acrchitectures and RPs			◔		◕	◑	◑	◑	◕	◔			◕	◕	◔
Management of AIs					◔			◑	◕	◔			◕	◑	
Dataset requirements and quality		◕		◑	◕		◑	◑	◔	◔			◑	◑	◔
Interoperability		◑			◕		◑	◑	◕	◔			◕	◑	◕
Test methodology and systems					◔		◕	◑					◕		◕
KPIs and conformance					◔						◔		◔		◔
System maturity assessment			◔		◔								◔		◕

Definitions for the terms used in the above table are:

- **Terminology:** vocabulary of technical terms in the particular field of AI
- **Use cases:** descriptions showing how AI enables or impacts a given functionality, service or test (including from a user's perspective)
- **Impact of EU ethics guidelines:** analyses how EU guidelines for AI could, should or shall impact specifications, standards or the standardization processes and the deployment of AI
- **Trustworthiness & Explainability of AI:** methods to enable humans to trace and interpret the reliability of AI results and also provide a human-understandable approximation of the causes of AI responses
- **Security/privacy:** functionality enabling restricted access to some data or services and potentially

also ensures the privacy of the data/service and/or its meaning within a selected small group

- **Architectures and RPs:** descriptions of how (and at what reference points) various AI functional elements interact with each-other and/or with other systems
- **Management of AIs:** the orchestration and full life-cycle of AI components i.e. how they are selected, onboarded, instantiated, trained, deployed, configured, monitored, updated and terminated when no longer needed
- **DataSet requirements and quality:** specifications that ensure that data elements entering AI systems can be correctly interpreted
- **Interoperability:** ability of a system or component to integrate and interwork with other component(s) or system(s) such that the interaction between the entities fully delivers the service described by the interface specification governing the interaction
- **Test methodology and systems:** means for executing the set of test cases that must be executed against a Component Under Test (CUT) or System Under Test (SUT) in order to pass verdicts on its functionality
- **KPIs and conformance:** measurable Key Performance Indicators to assess the behaviour/performance of the system, as well as conformance tests to determine whether the expected behaviour and performance criteria are met
- **System maturity assessment:** means of evaluation of stages in the introduction of AI systems, considering multi-dimensional criteria, scores, KPIs, etc. to evaluate the AI application and system, starting from systems with no AI and ending with fully AI-driven systems.

The above analysis shows an overview of the ongoing ETSI technical specifications related to AI. ETSI has historically supported societal issues within these and all its ICT standards. However, to ensure a prioritization of the ethical issues related to use of AI, ETSI and its members should also consider committing to an ethical mission statement: to develop standards that comply with the articles of the Universal Declaration of Human Rights [35] and therefore provide technical means to ensure appropriate privacy, trust and accountability in ICT systems.

It would be useful to apply the structure of Table 1 to the activities of relevant IEC, ITU and other groups, in a collaborative process, to identify potential synergies with ETSI work. Some examples of such groups are mentioned in the next section.

4 AI in other Organisations

4.1 Introduction

Many technical, regulatory and scientific groups are working on AI issues that may be either complementary or overlapping within the ICT space, where ETSI is active. This section provides a brief overview, and introduces possible collaboration partners. The ordering of the sections begins with discussion bodies, government policy and research bodies (advisory committees, research projects),

continues with independent open source and industry alliances, then finishes with a brief survey of national and international SDO groups.

4.2 Discussion Bodies

A large number of organisations related to AI have the mission to be “centres of discussion” for their members, for example:

- AI for Good: founded in April 2018 in France, it aims to put AI at the service of social innovation, with a focus on the environment, health and education
- AI Alliance Assembly: fostered by the EC, it provides a “whiteboard” for news and discussions
- AI Watch: setup by the EC, it monitors for Europe the development, uptake and impact of Artificial Intelligence, publishing dozens of reports, including the AI Index 2019
- Humans for AI: launched in 2019 in California, it aims to build the diverse workforce of the future, leveraging AI, interactions of diverse experts and practitioners and building on open source technologies
- European Centre for Living Technologies: monitors the ethics of artificial intelligence work.

4.3 Advisory Committees

Nearly all industrial nations have national policies on AI, with associated committees and reports. There is a blog overview of about 20 published national policies on AI, covering the period just to mid-2018 (see Dutton, Tim. "An Overview of National AI Strategies", published online 28th June 2018 [35]. The Japanese government published in March 2017 an Artificial Intelligence Technology Strategy (see Artificial Intelligence Technology Strategy. Report of Strategic Council for AI Technology, Japan [36]). The Chinese government published in June 2018 a White Paper on Artificial Intelligence Standardization, that has been partially translated into English (see Translation: Excerpts from China’s White Paper on Artificial Intelligence Standardization", published online 24th January 2018 [37]). The US published in February 2020 a report on the American AI initiative (see American Artificial Intelligence Initiative – year one annual report, published 25th February 2020 [38]).

The OECD set up a world-wide member expert group on AI, that identified a set of five principles (see OECD Recommendation of the Council on Artificial Intelligence", published 30th April 2020 [39]) for the responsible stewardship of trustworthy AI, and made five recommendations specifically towards governments. Those recommendations are also relevant to the development of standards for AI at ETSI

> (1) facilitate public and private investment in research & development to spur innovation in trustworthy AI;
>
> (2) foster accessible AI ecosystems with digital infrastructure and technologies and mechanisms to share data and knowledge;
>
> (3) ensure a policy environment that will open the way to deployment of trustworthy AI systems;
>
> (4) empower people with the skills for AI and support workers for a fair transition;

(5) co-operate across borders and sectors to progress on responsible stewardship of trustworthy AI.

Within Europe, there are a number of committees that are in a dialogue with regulators, such as:

- The EC HLEG on AI, that published in April 2019 the 'Ethics Guidelines for Trustworthy Artificial Intelligence' [1] followed in June 2019 by a document with 33 recommendations (see High-Level Expert Group. "Policy and investment recommendations for trustworthy Artificial Intelligence", Published 26th June 2019 [40]
- The Multi-stakeholder Platform, that is co-responsible for the EC Rolling Plan for ICT Standardization published it in March 2019 [12] and in March 2020 [41] with significant recommendations for AI.

4.4 Government Sponsored Research Projects

Within Europe, as also in the USA, China or India, etc., there are a number of government sponsored research programmes, which may impact AI technology, e.g. concerning explainability. The EU Horizon Europe research programme beginning in 2020 has a strong emphasis on AI and there are also many projects from the previous Horizon 2020 programme that are still delivering results, for example:

- AI4EU is a Horizon 2020 project that will bring together researchers, innovators and European talents who are currently working in the field of artificial intelligence
- Humane-AI is a Horizon 2020 project to design the principles for a new science that will make artificial intelligence based on European values
- LOGISTAR project proposes the intensive use of Internet of Things, Open Data, Artificial Intelligence, optimization techniques and other advances in ICT for effective planning and optimizing of transport in the logistics sector.

4.5 Open Source R&D

There are many small projects, however the following have significant impact:

- Linux Foundation AI Landscape provides an interactive overview of their open source projects, including Acumos AI for an AI marketplace, Adlik for ML optimization and AngelML for distributed ML
- Eclipse Deeplearning4J provides a set of modules for building AI applications
- TensorFlow is a core open source library to help develop and train machine learning models
- OpenAI is a non-profit research company releasing software regularly, based in San Francisco, with the goal to advance digital intelligence in the way that is most likely to benefit humanity.

4.6 Industry Alliances

A number of industry alliances are working on specifications for AI, or at least on gap analyses:

- TMForum AI & Data Analytics Project is addressing the following topics: (1) extending its data model to AI, (2) user stories and use cases, (3) service management for AI including APIs and an AI Checklist, (4) AI maturity model, (5) repository of AI data for training, (6) AIOPS
- BDVA has a number of working groups active in Big Data and AI (see AI Position Statement)
- GSMA supported the development of two major applied AI initiatives in 2019, aimed at sharing insight and developing an expert community: Applied AI Forum and the GSMA Global AI Challenge
- O-RAN alliance is considering RIC (RAN Intelligent Controller) and its relationship to AI

4.7 National and Regional standardization organisations

National standardization bodies often follow strategic priorities of their governments. Only a few examples are given below:

- CEN/CENELEC Focus Group on AI, in Europe, was launched in December 2018 based on the CEN-CENELEC Roadmap for AI Standardization [42] and is currently road-mapping AI standardization
- TTC in Japan has a group *AI for Next Generation Services* that plans the realization of a next-generation service platform using AI, starting with use cases for a cutting-edge business environment, including transparent and trustworthy AI/Machine Learning
- NIST in the USA has released a plan for prioritizing federal agency engagement in the development of standards for artificial intelligence in response to a government policy initiative (see "USA February 2019 Executive Order on Maintaining American Leadership on Artificial Intelligence (EO 13859) [43], documented it in the NIST AI standards website [44], and solicited comments in a public review [45] by organisations such as Microsoft, Intel, Google and many others [46].

4.8 Global SDOs

The global SDOs ITU and IEC/ISO have developed relevant standards and created several focus groups related to AI, many of which were highlighted during the March 2019 GSC-22 conference day on AI [47].

ISO/IEC

- ISO/IEC JTC1 SC42 Artificial Intelligence group is working on standards for the whole ecosystem of use cases (ISO/IEC NP TR 24030), ethics and governance (ISO/IEC AWI TR 24368, ISO/IEC AWI 38507), terminology (ISO/IEC WD 22989), big data (ISO/IEC AWI TR 20547-1) and bias (ISO/IEC NP TR 24027), big data and AI architecture (ISO/IEC DIS 20547-3.2, ISO/IEC WD 23053), risk management (ISO/IEC AWI 23894), trustworthiness and robustness (ISO/IEC PDTR 24028, ISO/IEC NP TR 24029-1)
- ISO/TC 184 Automation systems and integration group

ITU-T

- ITU-T SG13 has defined Y.3172 for declarative specification of Machine Learning applications
- ITU-T has a Focus Group on Machine Learning for Future Networks FG ML5G.
- ITU-T FG-AI4H is a collaboration of ITU with the WHO to form a Focus Group on artificial intelligence for health to establish a standardized assessment framework for the evaluation of AI-based methods for health, diagnosis, triage or treatment decisions.

IEEE

- IEEE P7000 addresses specific issues at the intersection of technological and ethical considerations, in system design, explainability of autonomous systems, data privacy, bias, terminology and ontologies, KPIs for face recognition.
- IEEE ECPAIS (Ethics Certification Program for Autonomous and Intelligent Systems) has the goal to create specifications for certification and marking processes that advance transparency, accountability and reduction in algorithmic bias in Autonomous and Intelligent Systems (A/IS).
- IEEE A-IS is the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems and has the mission to ensure every stakeholder involved in the design and development of autonomous and intelligent systems is educated, trained, and empowered to prioritize ethical considerations.

5 Recommendations: Future Directions on AI in ETSI

Artificial Intelligence is a game changer that brings several challenges to the ICT industry and to society in general. The use of AI as a tool needs to deal with interoperability and interchangeability issues, new concepts for testing and validation, and ensuring that ethics guidelines are embedded in order to guarantee a trustworthy Artificial Intelligence. Furthermore, it is yet to be fully evaluated what specific standardization needs may be required for Artificial Intelligence.

The full impact that AI technology may have in ETSI is yet to be determined, but several technical, strategic and external cooperation questions need to be address, requiring some coordination in the Institute.

The authors of this White Paper offer some recommendations for future work in ETSI, listed here and explained below:

- Coordinated approach to AI
- Complete mapping in ETSI of “AI as a tool”
- Evaluation of the technical impact of EU ethical guidelines
- AI Interoperability and Interchangeability
- Guidelines for AI Testing and Validation
- Dataset requirements and quality for Artificial Intelligence
- Partnership synergies

Coordinated approach to AI

Due to the strong growth in the use of AI, and the widespread activities in many SDOs and fora, there is a need to set priorities and promote manageable actions within ETSI. Below is a short list of potential opportunities for ETSI in the short/medium term, to increase ETSI's current AI footprint. The points need discussion and further elaboration within the overall ETSI community, as well as a "grass roots" voluntary participation. Organizational matters to achieve these objectives are out of the scope of this document, but are being addressed within the implementation of ETSI Long Term Strategy.

Complete mapping in ETSI of "AI as a tool"

Previous clauses in this White Paper have shown much activity in the ETSI community to include or develop AI systems in new standards. **A comprehensive and regularly updated map of "*Artificial Intelligence in ETSI*" should be completed with the help of all TBs/ISGs leaders and technical staff.** This could include both current approaches/activities as well as potential developments under discussion, especially if some work is deferred due to lack of voluntary competencies. This would help identify potential need for future Specialist Task Force projects in such areas, or suggest actions to increase education, communication and awareness. The map would also help in the definition of a common terminology and semantics for AI in ICT.

Compliance with the EU ethical guidelines

The EC HLEG Guidelines for a trustworthy AI (see Ethics Guidelines for Trustworthy AI, published 8th April 2019 [1]) includes seven requirement categories. Within the current structure of ETSI, each technical body would need to find means to apply the guidelines to their work related to AI, each one facing the same "learning curve". **ETSI should promote for AI an approach based on sharing and collaboration between groups**.

As a first step, **ETSI TBs should agree to analyse the technical methods proposed by HLEG for the assessment of a trustworthy AI**, whenever AI capabilities are referenced in ETSI standards.

To ensure a **prioritization of the ethical issues related to use of AI**, ETSI and its members should **consider committing to an ETSI ethical mission statement**, to develop standards that comply with the articles of the Universal Declaration of Human Rights [35] and the EC HLEG Guidelines [1] and the EU guidelines on ethics in artificial intelligence: Context and implementation [48] as they evolve].

AI Interoperability and Interchangeability

Interoperability and interchangeability are intrinsic benefits of a standardization process. This has led to the definition of physical/virtual interfaces, message flows, APIs, common data models within the standards, etc. When it comes to AI capabilities as part of new standards, **there is a need to revise these models, by identifying appropriate reference points, AI sub functions, levels of explicability of AI, quality metrics in the areas of human-machine and machine-machine interfaces, etc**. There may be potential to re-use some functional elements or protocols, after initial comparisons are made. Moreover, because AI models can introduce biases, AI interchangeability in complex systems could be a pragmatic way to (partially) manage the risk of bias. The **ETSI community should identify and analyse the best practices recommended by other SDOs** to tackle these problems in a complementary and collaborative manner.

Guidelines for AI Testing and Validation

As indicated by the EC HLEG on AI, and the EC's white paper on AI [14], "*due to the non-deterministic and context-specific nature of AI, traditional testing is not enough*". As explained in previous sections, there is an opportunity for ETSI (and in particular TC MTS together with TC INT) to **study and possibly generalize the available best practices and propose specification methods for AI capabilities in new standards, that are "testable" by design**, or to promote the use of AI to improve the traditional testing models as well management and selection of test suites. **The TC INT new WI on "Testing AI Models and AI in Test Systems", whose scope is already aligned with the aforementioned EC' recommendations (see EC white paper [14]), should be developed as a strong international reference for this topic**.

Dataset requirements and quality for Artificial Intelligence

Current AI technologies are based mainly on ML and on processing large amounts of data. This has led to a debate on data gathering, data ownership, data transparency, etc. that is going well beyond technical matters (privacy, regulation, remuneration schemes,…). The (negative) impact of poor quality training data is already very obvious, especially in Health applications, road travel, etc. Due to the growing use of AI models in standards, **ETSI Technical Bodies should investigate means to assess the "quality" of datasets** needed to train and also to test the AI capabilities referenced by new standards, expanding the work initiated by ISG SAI.

Partnership synergies

Over the years, ETSI has activated several dozens of partnerships with external SDOs, fora and research institutions. Many of these partners are already active in AI standardization as outlined in other chapters of this document. These partnerships should be employed to increase efficiency and improve the ETSI footprint on AI, by **promoting joint or complementary technical work, organizing common events**, or also to consider specific work for collaboration using the PAS scheme. This includes, as well, possible joint activities in AI Open Source projects where a recognized SDO like ETSI may bring additional value to the delivery of an open source implementation.

6 Conclusions

The increasing use of AI is impacting global business and private lives. It involves both huge opportunities and associated risks. Standardization is one means to efficiently and reliably exploit the opportunities, in Europe and globally.

This document surveys the many technical activities in ETSI that consider AI. They include 5G systems, network optimization, privacy/security, data management, semantic interoperability and testing across all areas. Each area is considering the use of aspects of AI, including Health and Human Factors scenarios. Increasing the visibility of ETSI work in AI areas and setting the links for a broader sharing of knowledge and solutions are key outcomes of this document.

A sampling of activities in other SDOs such as CEN/CENELEC, ISO/IEC, ITU, is included to provide context.

This White Paper makes clear that ETSI is working within many groups:

- to harness AI for optimization of ICT networks,
- to include ethical requirements in AI usage e.g. for eHealth, privacy/security
- to ensure reliability through appropriate testing of systems using AI,
- to overcome some AI-related security issues, and
- to better manage and characterize data, including from IoT systems, that is used by AI.

Increasing the collaboration with other standards groups, inside and outside of Europe, is a key recommendation of the authors for accelerating progress, reliability and trust in AI.

References

[1] High-Level Expert Group on AI. "Ethics Guidelines for Trustworthy AI". Published 8th April 2019. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

[2] "AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense". Published October 2019. https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF

[3] ETSI GR ENI 007 v1.1.1 (2019-11): "Experiential Networked Intelligence (ENI); Definition of Categories for AI Application to Networks", https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=56393

[4] "G20 Ministerial Statement on Trade and Digital Economy". Published 9th June 2019. https://www.mofa.go.jp/files/000486596.pdf

[5] "COM(2018) 795 final. Coordinated Plan on Artificial Intelligence". Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Published 07.12.2018. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56018

[6] EC. "Artificial Intelligence for Europe". COM(2018) 237 final. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Published 25th April 2018. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51625

[7] “Digital Europe Programme”. http://europa.eu/rapid/press-release_IP-18-4043_en.htm

[8] "OECD report on Private Equity Investment in Artificial Intelligence". Published 22nd January 2019. http://www.oecd.org/going-digital/ai/private-equity-investment-in-artificial-intelligence.pdf

[9] "OECD report on Artificial intelligence patents by top R&D companies, by headquarters' location, 2012-14". Published 22nd November 2017. https://read.oecd-ilibrary.org/science-and-technology/oecd-science-technology-and-industry-scoreboard-2017/artificial-intelligence-patents-by-top-r-amp-d-companies-by-headquarters-location-2012-14_sti_scoreboard-2017-graph25-en

[10] "Liability for Artificial Intelligence and other emerging digital technologies." Expert Group on Liability and New Technologies. Published 18th November 2019. https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608

[11] "EC Rolling Plan for ICT Standardization", Published March 2019. https://ec.europa.eu/docsroom/documents/34788/attachments/1/translations/en/renditions/native

[12] "Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (Text with EEA relevance)" https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R1150

[13] European Parliament. “A governance framework for algorithmic accountability and transparency”. Published 4th April 2019. https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2019)624262

[14] "WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust". COM(2020) 65 final. Published 19th February 2020. https://ec.europa.eu/info/files/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

[15] da Silva, Francisco, et. al., "The Impact of Artificial Intelligence and Autonomous Functions on the ETSI work-programme" in GSC-21 Vienna, 26-27 September 2017. https://www.itu.int/en/ITU-T/gsc/21/Documents/GSC-21_008_3_03_ETSI-R1.pptx

[16] “ETSI presentation on AI to the GSC-22”. Contributed 26th March 2019. https://www.itu.int/en/ITU-T/gsc/22/Documents/GSC-22-S05-002.pdf

[17] “ETSI Summit on Artificial Intelligence”. Published 4th April 2017. https://www.etsi.org/events/1474-etsi-summit-on-artificial-intelligence#pane-2

[18] ETSI TS 129 520 V15.0.0 (2018-07): "5G System; Network Data Analytics Services; Stage 3", https://www.etsi.org/deliver/etsi_ts/129500_129599/129520/15.00.00_60/ts_129520v150000p.pdf

[19] ETSI GS ZSM 002 , (2019-08): " Zero-touch network and Service Management (ZSM); Reference Architecture ", https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/002/01.01.01_60/gs_ZSM002v010101p.pdf

[20] ETSI GS ENI 001 v2.1.1 (2019-09): "Experiential Networked Intelligence (ENI); ENI use cases ", https://www.etsi.org/deliver/etsi_gs/ENI/001_099/001/02.01.01_60/gs_ENI001v020101p.pdf

[21] ETSI GS ENI 005 v1.1.1 (2019-09): "Experiential Networked Intelligence (ENI); System Architecture", https://www.etsi.org/deliver/etsi_gs/ENI/001_099/005/01.01.01_60/gs_ENI005v010101p.pdf

[22] ETSI TS 103.195-2 (2018-05): "Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture; Part 2: An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management ", https://www.etsi.org/deliver/etsi_ts/103100_103199/10319502/01.01.01_60/ts_10319502v010101p.pdf

[23] ETSI TS 103 194 (2014-10): "Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Scenarios, Use Cases and Requirements for Autonomic/Self-Managing Future Internet", https://www.etsi.org/deliver/etsi_ts/103100_103199/103194/01.01.01_60/ts_103194v010101p.pdf

[24] ETSI GS CIM 009 V1.2.1 (2020-02): "Context Information Management (CIM); NGSI-LD API; NGSI-LD v1.2.1", https://www.etsi.org/deliver/etsi_gs/CIM/001_099/009/01.02.01_60/gs_CIM009v010201p.pdf

[25] SAREF Smart Applications Reference Ontology. https://saref.etsi.org

[26] ETSI TS 103 327 V1.1.1 (2019-04): "Smart Body Area Networks (SmartBAN); Service and application standardized enablers and interfaces, APIs and infrastructure for interoperability management ", https://www.etsi.org/deliver/etsi_ts/103300_103399/103327/01.01.01_60/ts_103327v010101p.pdf

[27] ETSI GR ARF 001 V1.1.1 (2019-04): "Augmented Reality Framework (ARF); AR standards landscape", https://www.etsi.org/deliver/etsi_gr/ARF/001_099/001/01.01.01_60/gr_ARF001v010101p.pdf

[28] "ETSI ISG Securing Artificial Intelligence". Published 4th March 2020. https://portal.etsi.org/Portals/0/TBpages/SAI/Docs/2020-03-ETSI_SAI_Introduction.pdf

[29] "ETSI GANA Model in 5G Network Slicing, PoC White Paper #4". Published 27th August 2019, https://intwiki.etsi.org/images/ETSI_5G_PoC_White_Paper_No_4_v3.1.pdf

[30] ETSI EG 203 341 V1.1.1 (2016-10): "Core Network and Interoperability Testing (INT); Approaches for Testing Adaptive Networks", https://www.etsi.org/deliver/etsi_eg/203300_203399/203341/01.01.01_60/eg_203341v010101p.pdf

[31] "WHITEPAPER #5: Artificial Intelligence (AI) in Test Systems, Testing AI Models and ETSI GANA Model's Cognitive Decision Elements (DEs) via a Generic Test Framework for Testing GANA Multi-Layer Autonomics & their AI Algorithms for Closed-Loop Network Automation". Published 29th March 2020. https://intwiki.etsi.org/images/ETSI_5G_PoC_White_Paper_No_5.pdf

[32] ETSI Whitepaper #4: "ETSI GANA Multi-Layer Autonomics & their AI Algorithms for Closed-Loop Network Automation", https://intwiki.etsi.org/images/ETSI_5G_PoC_White_Paper_No_4_v3.1.pdf

[33] "Modern Hippocratic Oath holds the underlying values of medicine in a digital world ". Published 13th July 2018. https://medschool.ucla.edu/body.cfm?id=1158&action=detail&ref=1056

[34] United Nations. "Universal Declaration of Human Rights". https://www.un.org/en/universal-declaration-human-rights

[35] Dutton, Tim. "An Overview of National AI Strategies". Published online 28th June 2018. https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd

[36] "Artificial Intelligence Technology Strategy. Report of Strategic Council for AI Technology, Japan. Published 31st March 2017. https://www.nedo.go.jp/content/100865202.pdf

[37] "Translation: Excerpts from China's White Paper on Artificial Intelligence Standardization". Published online 24th January 2018. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-excerpts-chinas-white-paper-artificial-intelligence-standardization/

[38] "American Artificial Intelligence Initiative – year one annual report", Published 25th February 2020. https://www.whitehouse.gov/wp-content/uploads/2020/02/American-AI-Initiative-One-Year-Annual-Report.pdf

[39] "OECD Recommendation of the Council on Artificial Intelligence". Published 30th April 2020. https://legalinstruments.oecd.org/api/print?ids=648&lang=en#:~:text=The%20Recommendation%

20aims%20to%20foster,human%20rights%20and%20democratic%20values.&text=In%20June%202019%2C%20at%20the,drawn%20from%20the%20OECD%20Recommendation

[40] High-Level Expert Group. "Policy and investment recommendations for trustworthy Artificial Intelligence", Published 26th June 2019. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60343

[41] "EC Rolling Plan for ICT Standardization". Published March 2020. Updated 5th June 2020. https://ec.europa.eu/docsroom/documents/41541/attachments/1/translations/en/renditions/native

[42] "CEN-CENELEC Roadmap for AI Standardization". Submitted 24th January 2019. ftp://ftp.cencenelec.eu/EN/News/SectorNews/2019/AI-Focus-Group/CEN-CLC_AI_FGN004_Roadmap.pdf

[43] "USA February 2019 Executive Order on Maintaining American Leadership on Artificial Intelligence (EO 13859)". https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/

[44] "NIST Resource Page on AI". https://www.nist.gov/topics/artificial-intelligence/ai-standards

[45] "Comments Received for RFI about Federal Engagement in Artificial Intelligence Standards". https://www.nist.gov/topics/artificial-intelligence/comments-received-rfi-about-federal-engagement-artificial

[46] See: ANSI https://www.nist.gov/system/files/documents/2019/06/06/nist-ai-rfi-ansi-001.pdf, OpenAI Alliance https://www.nist.gov/system/files/documents/2019/06/10/nist-ai-rfi-openai-001.pdf, Microsoft https://www.nist.gov/system/files/documents/2019/06/10/nist-ai-rfi-microsoft-001.pdf, Google https://www.nist.gov/system/files/documents/2019/06/10/nist-ai-rfi-google-001.pdf, Intel https://www.nist.gov/system/files/documents/2019/06/11/nist-ai-rfi-intel-001.pdf

[47] Global Standards Collaboration, 26-27 March 2019, Montreux, Switzerland, GSC-22 Meeting Documents. https://www.itu.int/en/ITU-T/gsc/22/Pages/documents.aspx

[48] "EU guidelines on ethics in artificial intelligence: Context and implementation". Published 19th September 2019. http://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf

Work Items underway in ETSI

The following are work items mentioned within this White Paper which are currently underway without yet achieving full publication status.

[wi 1] ETSI DGR/NFV-IFA041 (in draft): "Network Functions Virtualisation (NFV); Release 4 Management and Orchestration; Report on enabling autonomous management in NFV-MANO; Autonomous mgmt in MANO". https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58467

[wi 2] ETSI TR 103 674 (in draft): "SmartM2M; Artificial Intelligence and the oneM2M architecture", https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=57866

[wi 3] ETSI TR 103 675 (in draft): "SmartM2M AI for IoT: A Proof of Concept; PoC AI4IoT" https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=57867

[wi 4] ETSI DGR/CIM-007-SEC (in draft): " Context Information Management (CIM); Security and Privacy", https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=53370

[wi 5] ETSI AR DGS/ARF-003 (2020-03): "Augmented Reality Framework (ARF); AR framework architecture". https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=54070

[wi 6] ETSI DGR/SAI-004 "Securing Artificial Intelligence (SAI); Problem Statement; SAI Problem Statement ", https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=59209

[wi 7] ETSI DGR/SAI-001 "Securing Artificial Intelligence (SAI); AI Threat Ontology AI Threat Ontology", https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58856

[wi 8] ETSI DGR/SAI-002 "Securing Artificial Intelligence (SAI); Data Supply Chain Report; Data Supply Chain Report", https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58857

[wi 9] ETSI DGR/SAI-005 "Securing Artificial Intelligence (SAI); Mitigation Strategy Report; SAI Mitigation Strategy report", https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=59214

[wi 10] ETSI DGS/SAI-003 "Securing Artificial Intelligence (SAI); Security Testing of AI; Security Testing of AI", https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58860

[wi 11] ETSI TR 103 821 (DTR/INT-008_AFI AI Testing) “Autonomic network engineering for the self-managing Future Internet (AFI); Artificial Intelligence (AI) in Test Systems and Testing AI models. Artificial Intelligence (AI) in Test Systems”. https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58442

[wi 12] ETSI TS 102 182 v1.4.6 (in draft): "Emergency Communications (EMTEL); Requirements for communications from authorities/organizations to individuals, groups or the general public

during emergencies",
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=57466

[wi 13] ETSI TS 102 181 v1.2.11 (in draft):" Emergency Communications (EMTEL); Requirements for communication between authorities/organizations during emergencies between authorities "
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58056

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org