ETSI The Standards People

Steps Required Towards Building Standards-based Testbeds and Frameworks for Certifications of AI Models / Components / Systems

Dr Tayeb Ben Meriem, Orange
Dr Andreas Ulrich, Siemens

ITU ETSI IEEE Joint SDOs Brainstorming Workshop on Testbeds Federations for 5G & Beyond: Interoperability, Standardization, Reference Model & APIs

March 16th 2021

What We Do

ETSI TC INT (Core Network and Interoperability Testing)

- Develops core network test specifications for conformance, interoperability, performance etc. and supervises interoperability events

ETSI TC MTS (Methods for Testing and Specification)

- Defines specification and testing methods for use in the development of standards, incl. test description language TDL, test execution language TTCN-3 and frameworks

ETSI via TC INT and TC MTS is the Home for Test & Certification of AI Models and Autonomic/Autonomous Networks activities

Achievements on Testing Autonomic Networks and AI

2021	ETSI TC INT/MTS Technical Reports on “Benefits of AI in Testing” and “Testing of AI Models, Components, and Systems with Quality Metrics” (publication planned)
2020 Jul	ETSI White Paper #34 on “Artificial Intelligence and future directions for ETSI”
	ETSI TC INT / ITU-T SG 11 Joint New Work Item “Federated Testbeds”
2020 Mar	5G Proof of Concept (PoC) White Paper #5, “AI in Test Systems, Testing AI Models and ETSI GANA Model's Cognitive Decision Elements (DEs)”
2020 Feb	European Commission’s recommendations on Testing and Certification of AI and mapping with ETSI TC INT AI-Support System
2019	Creation of a joint ETSI TC INT/MTS New Work Item “AI in Test Systems and Testing AI Models”
2016	ETSI Guide ETSI EG 203 341 V1.1.1 “Approaches for Testing Adaptive Networks”

ETSI Work Is Aligned with the EC's Recommendations on Testing and Certifying AI

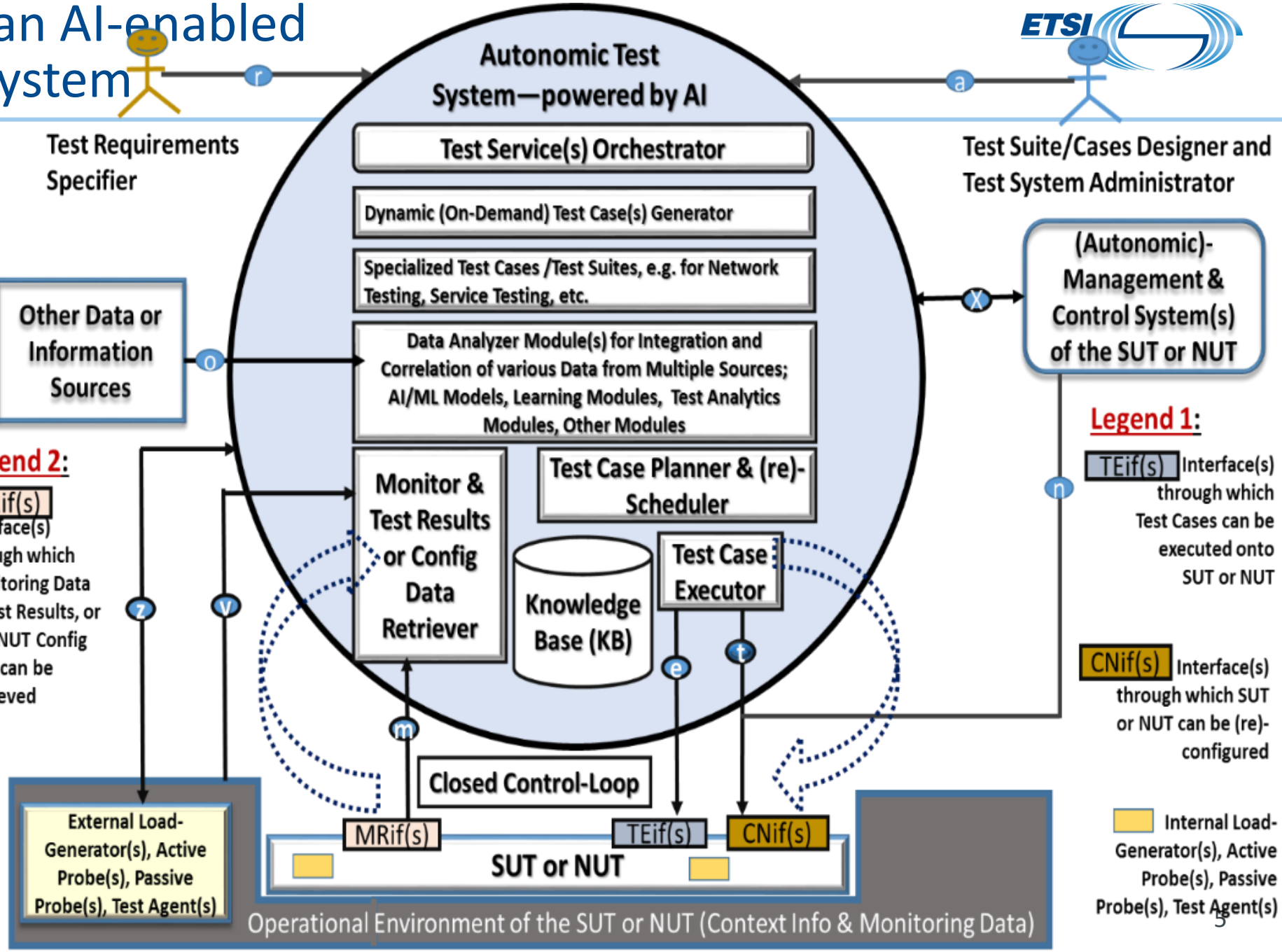
EC White Paper on "Artificial Intelligence: a European approach to excellence and trust", 19-Feb-2020 emphasises the need for

1. A regulatory framework,
2. The creation of an AI test centre, and
3. The creation of a certification centre.

The ETSI framework on "**AI Testing & Certification**", proposed in White Paper #5, aims at the translation of the three recommendations into operational tools covering

- Standardisable metrics for measurements and assessments in testing and certifying AI models within autonomic networks
- Methodologies and customisable frameworks for test system providers and certification authorities

Concept View of an AI-enabled Autonomic Test System



AI and Trustworthiness

Trustworthiness of AI, i.e. the AI shall be demonstrably worthy of trust, covers at least the three aspects*:

- It should be **lawful**, complying with all applicable laws and regulations;
- It should be **ethical**, ensuring adherence to ethical principles and values; and
- It should be **robust**, both from a technical and social perspective.

Focus of work

*) High-Level Expert Group on Artificial Intelligence: Ethics Guidelines for Trustworthy AI, 2019

Quality Metrics for AI-enabled Systems

Today, AI is dominated by Machine Learning (ML) techniques

- Mathematical models used to extract information from large data sets

There is a need for **metrics** to capture and assess quality characteristics of ML models

- Probabilistic **accuracy** under uncertainty
- Technical **robustness** against noisy, erroneous, or (constructed) adversarial data
- Others: reliability, fairness, safety, security, explainability

	Actually Positive	Actually Negative
Predicted Positive	True Positive	False Positive
Predicted Negative	False Negative	True Negative

Confusion matrix measures the performance of ML model

Tackling the Technical Aspects of Certifying ML Models

Different ML models require different approaches to testing

	Offline Learning	**Continuous Learning**
State-full	Recurrent Neural Networks	Re-enforcement learning
State-less	Feedforward Neural Networks, Bayesian Networks	Generative Adversarial Networks

Challenges:
Expressing uncertainties in test scenarios; test coverage and test end criteria; test oracle; data quality for training and test (e.g. bias, noise); interoperability of ML models; online testing during production

Backup

Artificial Intelligence and future directions for ETSI (WP#34)

◔ = 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			◔		◔								◔		◕

ETSI aims to handle specific needs for AI:

- 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.

https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp34_Artificial_Intelligence_and_future_directions_for_ETSI.pdf