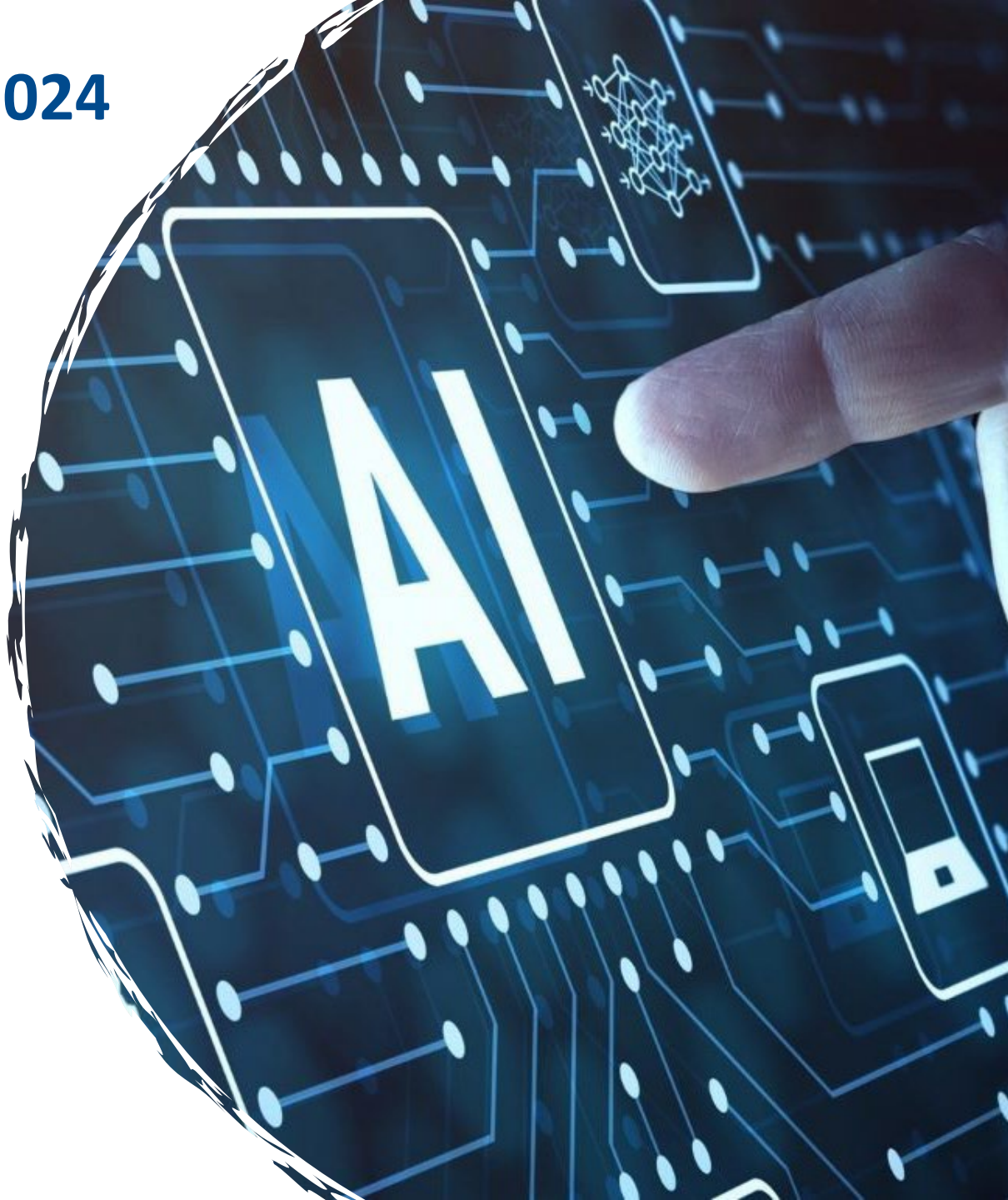
ETSI AI Conference 2024



Cooperation between ETSI and JTC21

Presented by:

Dr. Markus Mueck

ETSI OCG-AI Chair,
ETSI Board Chair

05/02/2024

Overview

- ETSI Operational Co-ordination Group on Artificial Intelligence (OCG AI) coordinating alignment with European Commission, CEN/CENELEC JTC21, etc.
- ETSI's activities in the field of Artificial Intelligence of potential relevance to the implementation of the European AI Act
- Dialogue & collaboration between ETSI and CEN/CENELEC JTC21
- Conclusions and next steps

ETSI Operational Co-ordination Group on Artificial Intelligence (OCG AI)

ETSI OCG AI is open to all ETSI members. Its tasks include

- To facilitate the exchange of views and information on AI activities in Technical Bodies (TBs) and Industry Specification Groups (ISGs) in order to identify synergies, best practices and common requirements and
- To coordinate provision of information by the TBs and ISGs on AI matters relevant to ETSI.

ETSI OCG AI is representing ETSI in regular EC / ESOs meetings where the European Commission, ETSI and CEN/CENELEC exchange information on the latest status of activities related to the European AI Act and AI in general.

All ETSI members are invited to join OCG AI
which provides an holistic view on ETSI's activities in the field of AI!

ETSI's activities in the field of AI of potential relevance to the implementation of the European AI Act

ETSI has published a White Paper outlining available ETSI work of potential relevance for the implementation of the European AI Act:

ETSI White Paper No. #52
ETSI Activities in the field of Artificial Intelligence
Preparing the implementation of the European AI Act

The White Paper summarizes ongoing and planned ETSI activities in the field of AI:

- Human Factors requirements related to transparency, information to the users, and human oversight of AI systems;
- Glossary and Standards Landscape;
- AI Robustness, Trust & Confidence Building in AI-powered systems, and Test & Certification of selected class(es) of AI-powered systems;
- Testing-based conformity assessment for AI-enabled systems;
- Cognitive Management of AI Systems;
- Etc.

https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP52-ETSI-activities-in-the-field-of-AI-B.pdf

Dialogue between ETSI and CEN/CENELEC JTC21

CEN and CENELEC have established the CEN-CENELEC Joint Technical Committee 21 **'Artificial Intelligence'.**

ETSI and CEN/CENELEC JTC21 are collaborating closely.

The collaboration includes:

- **Participation by ETSI to CEN/CENELEC JTC21 meetings in the context of a Collaboration Agreement;**
- **Participation of ETSI experts in CEN/CENELEC JTC21 Working Groups;**
- **Recommendation on relevant ETSI work for referencing in CEN/CENELEC JTC21 deliverables.**

Dialogue between ETSI and CEN/CENELEC JTC21, Cont'd

A dialogue is ongoing between ETSI ISG SAI (now TC SAI) and JTC21 to discuss available deliverables of relevance to the implementation of the European AI Act. A corresponding Liaison Statement was issued in 2023:

A specific recommendation was given by the Liaison Statement as follows:

"In particular, ETSI ISG SAI asks that the work on AI Transparency undertaken in JTC21 references the publications from ETSI (GR SAI 007) and takes into account the work in progress (Draft GR 010)."

2. Summary of ETSI ISG SAI work programme

The scope of ETSI's ISG SAI work programme is fairly extensive and has resulted in a number of important publications. Of particular note are the most recent publications of ETSI ISG SAI made in the first months of 2023:

ETSI GR SAI 007 V1.1.1 (2023-03): Securing Artificial Intelligence (SAI); Explicability and transparency of AI processing
The scope of GR SAI 007 identifies the content as identifying steps to be taken by designers and implementers of AI platforms that give assurance of the explicability and transparency of AI processing. AI processing includes AI decision making and AI data processing. The document identifies its target audience as designers and implementers who are making assurances to a lay person. In more detail the content addresses both static and dynamic forms in order to allow designers to be able to "*show their working*" (explicability) and to be "*open to examination*" (transparency)
ETSI GR SAI 009 V1.1.1 (2023-02): Securing Artificial Intelligence (SAI); Artificial Intelligence Computing Platform Security Framework
The scope of GR SAI 009 states that it describes a security framework of AI computing platform containing hardware and basic software to protect valuable assets like models and data deployed on AI computing platform when they are used in runtime or stored at rest. The security framework consists of security components in AI computing platform and security mechanisms executed by security components in the platform. By specifying the security framework, an AI computing platform can be consolidated against the relevant attack and can provide security capabilities to facilitate the stakeholders in AI systems to better protect the valuable assets (model/data) on an AI computing platform.
ETSI GR SAI 013 V1.1.1 (2023-03): Securing Artificial Intelligence (SAI); Proofs of Concepts Framework

https://docbox.etsi.org/OCG/OCG_AI/05-CONTRIBUTIONS/2023/OCGAI(23)032003_Liaison_Statement_from_ETSI_ISG_SAI_to_JTC21_on_recent_work_.pdf

Dialogue between ETSI and CEN/CENELEC JTC21, Cont'd

TC SAI will inherit and maintain the work done under the auspices of ISG SAI.

TC SAI addresses 4 main aspects of AI security standardisation:

1. Securing AI from attack e.g. where AI is a component in the system that needs defending;
2. Mitigating against AI e.g. where AI is the 'problem' (or used to improve and enhance other more conventional attack vectors);
3. Using AI to enhance security measures against attack from other things e.g. AI is part of the 'solution' (or used to improve and enhance more conventional countermeasures);
4. Societal security and safety aspects of the use and application of AI.

- TC SAI will produce both informative documents (Technical Reports (including Special Reports and ETSI Guides)) and normative documents (Technical Specifications (including ENs and if requested hENs)).
- In addition TC SAI will inherit and maintain the work done under the auspices of ISG SAI.
- In addressing secure AI with the broad interpretation of security to include safety and societal aspects as above TC SAI will engage with EU and other regulatory bodies to ensure that the output supports relevant global, regional and national requirements.

Dialogue between ETSI and CEN/CENELEC JTC21, Cont'd

In a dialogue between ETSI and CEN/CENELEC, additional opportunities have been identified, including:

Possible work by ETSI may relate to

- Solutions on "Traceability/Lineage of Data";
- Solutions on "Traceability of AI Models";
- Solutions on "Explicability and transparency of AI processing";
- ETSI references to be included into JTC21's "AI Trustworthiness framework";
- Etc.

Next Steps

- ETSI has substantial work available and ongoing in the field of Artificial Intelligence;
- ETSI is supporting the implementation of the European AI Act exploiting its activities on Artificial Intelligence;
- ETSI is closely collaborating with CEN/CENELEC JTC21 to support the implementation of the European AI Act.

Thank you for your attention

Follow us on:

Any further questions?

Contact me:

Markus.Dominik.Mueck@intel.com