GISC 2025

Global ICT Standards Conference 2025

Enabling the physical AI era with global standards

European approach to the Physical AI and Standardization Direction

Scott CADZOW
Chair TC SAI, ETSI

ICT Standards and Intellectual Property:
AI for All

Hosted by Ministry of Science and ICT, Ministry of Intellectual Property
Organised by National Radio Research Agency, TTA, IITP, KEA, kista, ETRI

Index

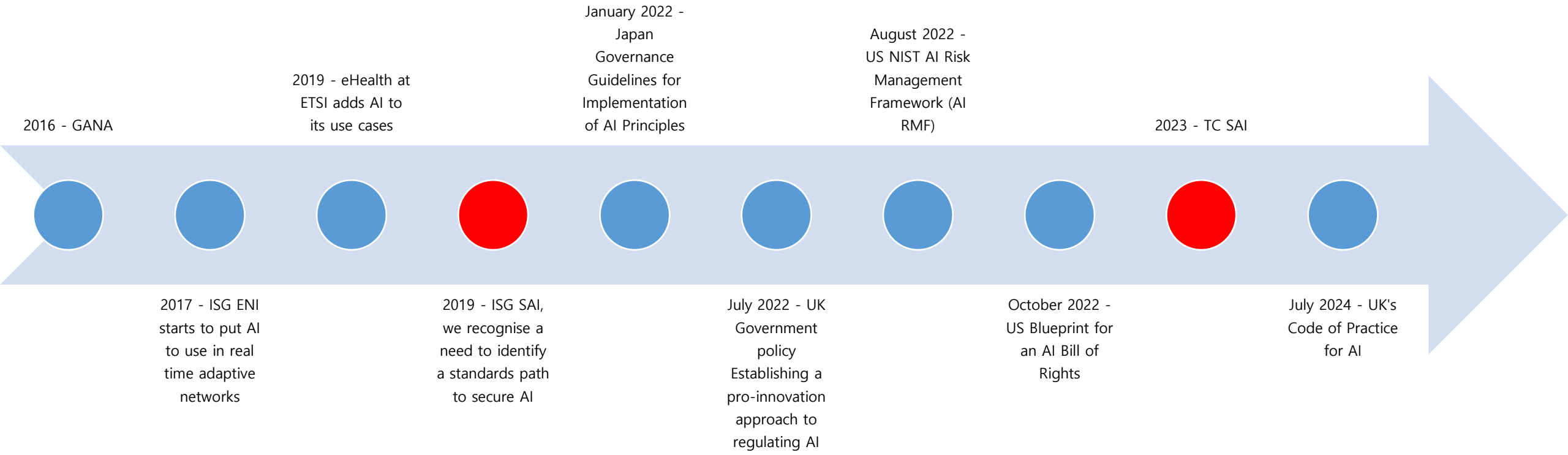
Abstract

European standards in AI - a view from ETSI

AI Standards

An overview, primarily from the perspective of ETSI, of standards to secure and assure safe use of AI. The metric for success in standardization is proposed and outlined. The presentation addresses the ETSI approach of consensus building. It highlights the work done in the last 6 years where AI has been an active topic in ETSI and outlines the content of the standards published and the ones in development. It also identifies future areas where standards are planned and where global cooperation is essential for success

01. A timeline of AI standards and governance milestones



02. General approach to standardization in ETSI

There are 3 distinct steps in standards development that address all 5 phases of the market

Problem identification

- What is the problem to be solved?

Solution research

- Does a solution exist? Is it viable?

Solution specifications

- The mitigations, the provisions

Different deliverable types distinguish the steps:

- Reports and Guides cover the identification and research steps
  - GRs, TRs, EGs
- Technical specifications address the solution step
  - TSs, ESs, ENs

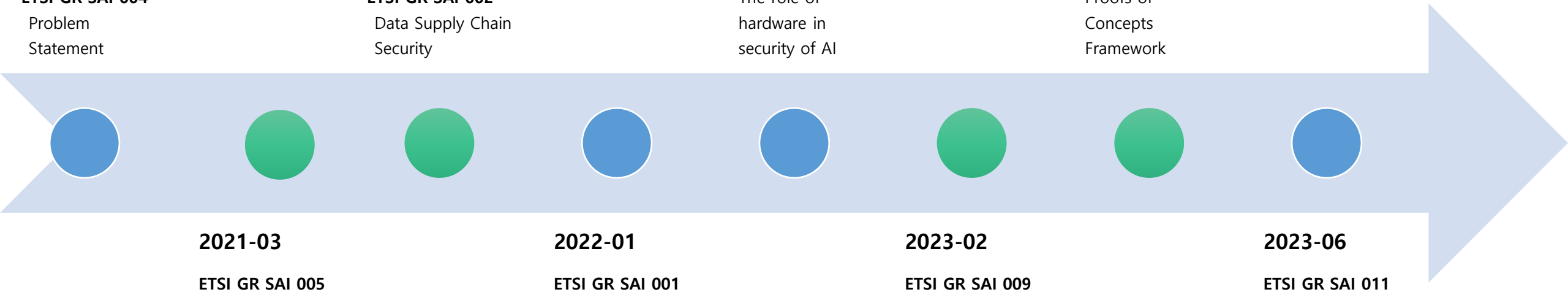
The approval process is the only significant difference between (say) a TS, ES and EN

Design Development Deployment Maintenance End-of-life

03. What does “S” in SAI mean or signify?

ETSI’s Technical Committee Securing Artificial Intelligence (TC SAI) deliberately overloads the “S” in SAI. Whilst it can be first interpreted as Secure in the meaning of cyber-security and the application of the well known Confidentiality-Integrity-Availability (CIA) paradigm, it also addresses safety in the meaning of designing AI systems to be intrinsically safe (i.e. taking a similar view of AI as we do in the domain of Functional Safety in other engineering disciplines), and we also want AI to be societally relevant. This last ensures that we address how AI impacts people, societies, industries and nations. It allows us to take steps to consider the human impact of AI and how we can mitigate negative consequences of its use.

04. ETSI SAI publication timeline (ISG SAI era)



2020-12

ETSI GR SAI 004
Problem Statement

2021-03

ETSI GR SAI 005
Mitigation Strategy Report

2021-08

ETSI GR SAI 002
Data Supply Chain Security

2022-01

ETSI GR SAI 001
AI Threat Ontology

2022-03

ETSI GR SAI 006
The role of hardware in security of AI

2023-02

ETSI GR SAI 009
Artificial Intelligence Computing Platform Security Framework

2023-03

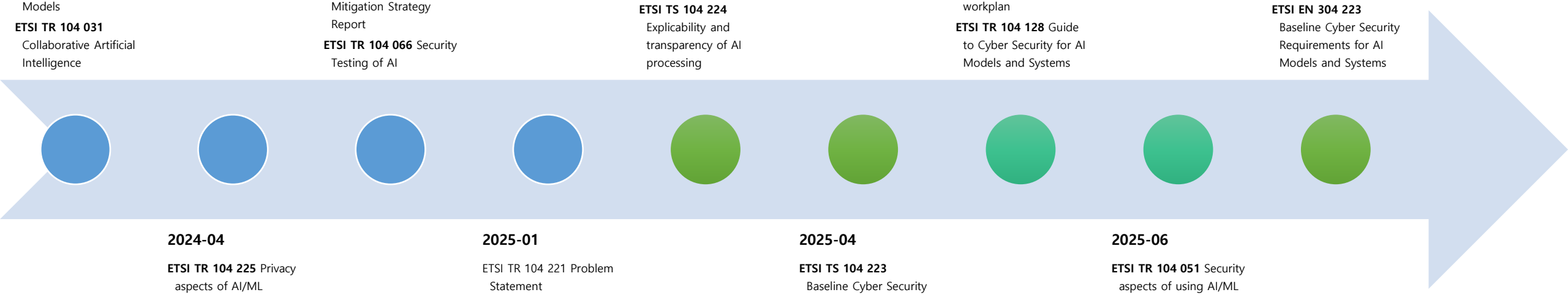
ETSI GR SAI 007
Explicability and transparency of AI processing

ETSI GR SAI 013
Proofs of Concepts Framework

2023-06

ETSI GR SAI 011
Automated Manipulation of Multimedia Identity Representations

05. The wider standards picture in Europe for AI



2024-02

ETSI TR 104 032 Traceability of AI Models

ETSI TR 104 031 Collaborative Artificial Intelligence

2024-04

ETSI TR 104 225 Privacy aspects of AI/ML systems

ETSI TR 104 067 Proofs of Concepts Framework

2024-07

ETSI TR 104 062 Automated Manipulation of Multimedia Identity Representations

ETSI TR 104 222 Mitigation Strategy Report

ETSI TR 104 066 Security Testing of AI

2025-01

ETSI TR 104 221 Problem Statement

ETSI TR 104 048 Data Supply Chain Security

2025-03

ETSI TR 104 030 Critical Security Controls for Effective Cyber Defence; Artificial Intelligence Sector

ETSI TS 104 050 AI Threat Ontology and definitions

ETSI TS 104 224 Explicability and transparency of AI processing

2025-04

ETSI TS 104 223 Baseline Cyber Security Requirements for AI Models and Systems

2025-05

ETSI TR 104 065 AI Act mapping and gap analysis to ETSI workplan

ETSI TR 104 128 Guide to Cyber Security for AI Models and Systems

2025-06

ETSI TR 104 051 Security aspects of using AI/ML techniques in telecom sector

2025-09

ETSI EN 304 223 Baseline Cyber Security Requirements for AI Models and Systems

06. The wider AI eco-system

This is captured and updated in ETSI's TR 104 029.

Taken from Annex B: AI security relationship diagrams of TR 104 029 and expanded upon in subsequent slides

Market Requirements	•Autonmous vehicles levels 4 to 6; Robotic & Machine Intelligence •Telecomunications Infrastructure and Services - Autonomous Networking and Optimisation •Utility Networks and Services; Industrial Systems •Biometric; Health Services •Finanical Services; User Experiance; Education
Regulation & Legislation	•EU AI Act; Council of Europe - AI Convention •Germany - German Standardization Roadmap for Artificial Intelligence" (NRM KI) ; UK - AI Cyber Security Code of Practice •USA - Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence; Utah, USA - Artificial Intelligence Policy Act; Tennessee, USA Ensuring Likeness Image and Voice Security (ELVIS) Act; Calinfornia, USA - Safe and Secure Innovation for Frontier Artificial Intelligence Models Act.
NGOs & GOs Advisors on AI	•MITRE ATLAS ((Adversarial Threat Landscape for Artificial-Intelligence Systems) •NIST - societal, ethics, governance & privacy •OAWSP •ENISA; EC AI HLEG; European Centre for Algorithmic Transparency (ECAT) inside JRC •FIRST
Standards Development Organisations	•ETSI OCG AI; TC SAI; ISG ENI; ISG ZSM •CEN-CENELEC JTC 21 •ISO/IEC JTC 1 SC 42; IEC SEG 10 •SAC/TC 260 #AI •ITU-T: 13 future networks; 16 multimedia; 17 Security; 20 IoT/Smart Cities; 2 operations; 15 transport
Security Functions	•Zero Trust Model for AI •AI Bill of Materials ; Data Supply Chain; Data Integrity during Acquition and Curation •Hardware to Secure AI - Gateway/Middlebox •Security testing of AI •Threat Landscape for AI Cybersecurity ; AI for Cyber Crisis Management •AI - Risk Management; Trustworthiness in AI •Test adequacy criteria/test stop criteria; Testing techniques to protect access to data and input sensor data (e.g. video, etc)

07. Collaborative standards actions in ETSI and amongst SDOs

Load is shared amongst SDOs and collaboration meetings, liaisons, shared memberships, work to address any potential conflict.

Standards Development Organisations

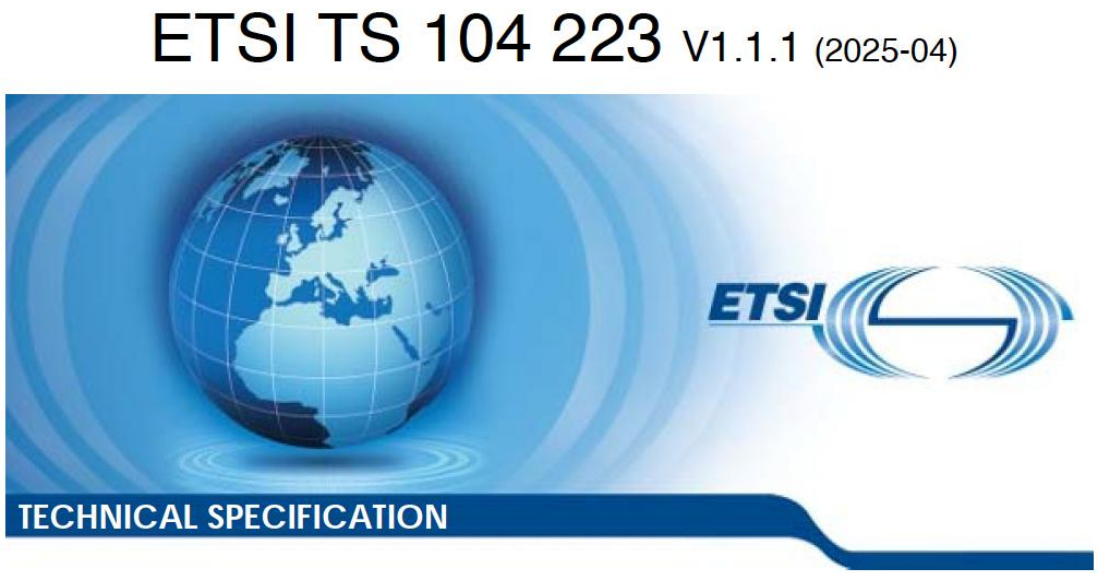
- ETSI OCG AI; TC SAI; ISG ENI; ISG ZSM
- CEN-CENELEC JTC 21
- ISO/IEC JTC 1 SC 42; IEC SEG 10
- SAC/TC 260 #AI
- ITU-T: 13 future networks; 16 multimedia; 17 Security; 20 IoT/Smart Cities; 2 operations; 15 transport

08. What is the plan from ETSI for AI standardization?

Establish a baseline for all AI

This is captured in the baseline principles for AI security in ETSI TS 104 223 (and to come EN 304 223):

13 core design principles
A total of 72 trackable provisions
5 lifecycle phases.



09. The next steps in AI standards at ETSI

Addressing and filling gaps -- identifying problems, developing solutions

- TR 104 097 -- AI and safety -- Functional Safety in AI-dev
- TS 104 225 -- Privacy -- Addressing AI privacy normatively
- TS 104 158-1 (now in 4 parts) -- AI and vulnerability reporting -- AICIE
- TR 104 159 -- AI and social responsibility
- TS 104 216 -- Metrics and testing of AI

10. AI and safety -- Functional Safety in AI-dev

TR 104 097 -- Guide to the secure by design considerations and assurance in AI systems development

The intent of this work item is to identify the actions of AI developers to ensure that their products and systems remain safe and secure when deployed. This work item will report on the core measures and how they work alongside the core principles of SAI. The intent is to ensure systems are both secure and safe in the deployed context. This reinforces secure by design. To also address how to give assurance of a secure and safe design.

Reinforces the design, deployment and maintenance phases

Design Development **Deployment** **Maintenance** End-of-life

11. AI and Privacy -- Addressing AI privacy normatively

TS 104 225 -- Privacy aspects of AI/ML systems

The intent of this work is to take the text of TR 104 225 and to extend it to make normative provisions addressing privacy and data protection. This will address aspects including "the right to be forgotten" and how to ensure if data is removed from an AI system that it is not recoverable.

NOTE: this will replace the TR by making normative provisions

Reinforces the design, development and end-of-life phases

Design **Development** Deployment Maintenance **End-of-life**

10. AI and vulnerability reporting -- AICIE

TS 104 158-1 -- AI Common Incident Expression (AICIE)

The intent of this work is to provide AI Common Incident Expression together with a Common Incident Scoring System that is compatible with lightweight information exchange standards.

Intended to bind AI into the same vulnerability reporting schemas as used in TC CYBER, FIRST, NIST and many others

Reinforces the deployment, maintenance and end-of-life phases

Design Development **Deployment** **Maintenance** **End-of-life**

10. AI and social responsibility

TR 104 159 -- Understanding and Preventing Harm from Generative AI

The intent of this work is to provide an understanding of the harm from Generative AI along with presenting the different ways to prevent that harm. This includes but is not limited to malicious code generation, deepfakes, spam messages, disinformation etc. The areas also covered are the issues of AI hallucinations, loss of confidentially and IPR infringements. The types of methods to counter the harm from Generative AI to be considered in the report are detection, enforcement, reporting and removal.

Reinforces the design, deployment and maintenance phases

Design Development **Deployment** **Maintenance** End-of-life

10. AI and safety -- Metrics and testing of AI

TS 104 216 -- Conformance assessment for AI (EN 304 223)

In very simple terms the intent of this work is to define methods for assessing conformance to EN 304 223. In practical terms the much wider intent of this work is to develop methods that allow testing to work in order to both aid conformance and to set proper metrics.

This work is supported by many "weights and measures" experts.

Reinforces the design, development and deployment phases

Design **Development** **Deployment** Maintenance End-of-life

GISC 2025

Global ICT Standards Conference 2025

- Thank you -

Scott CADZOW, Chair ETSI TC SAI

scott@cadzow.com

ICT Standards and Intellectual Property:
AI for All

Hosted by Ministry of Science and ICT, Ministry of Intellectual Property

Organised by National Radio Research Agency, TTA, IITP, KEA, kista, ETRI