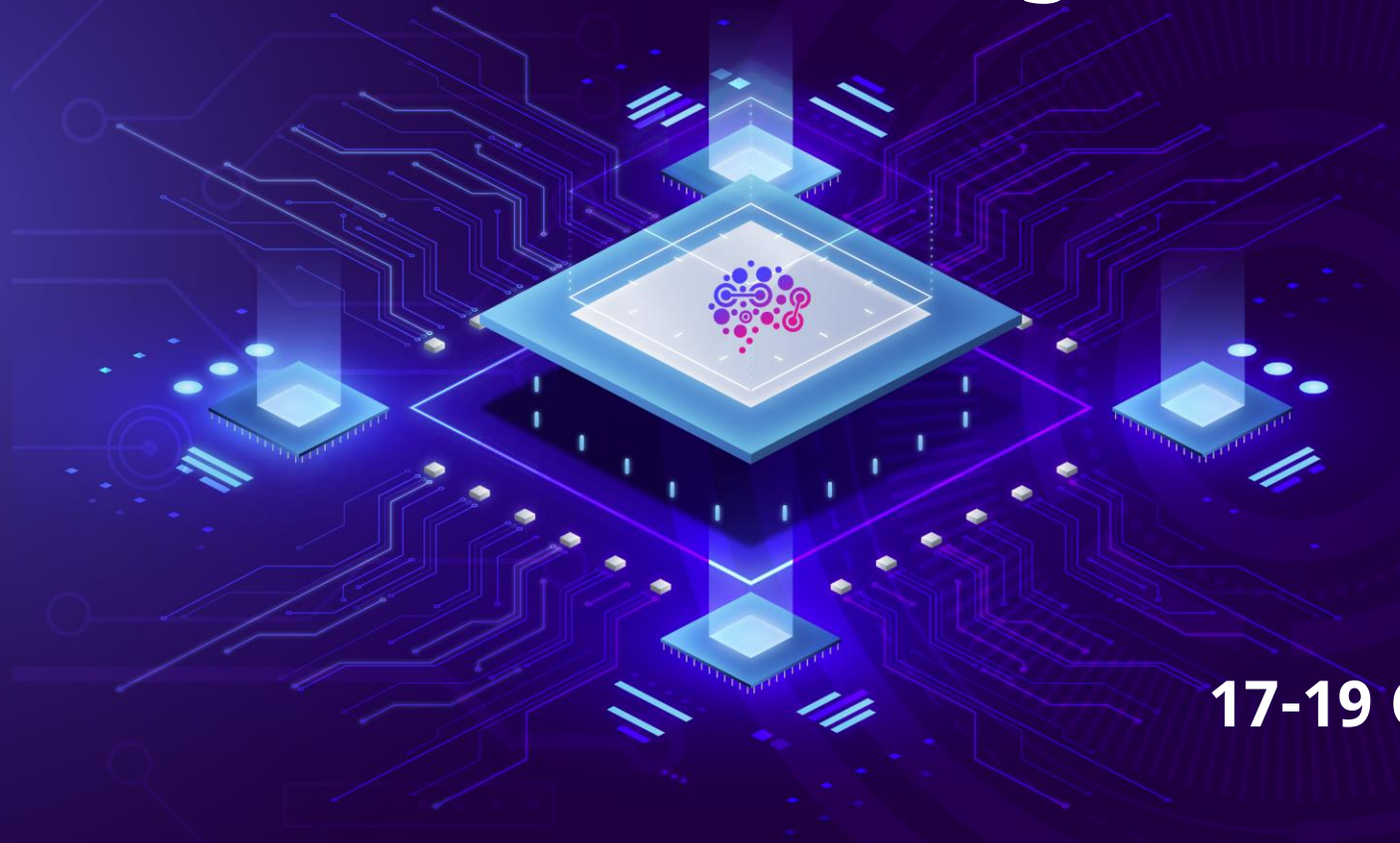
EDGE AI

European Conference on EDGE AI Technologies and Applications - EEAI



Advancing emerging edge AI technologies and driving next generation intelligent applications.

17-19 October 2023, Athens, Greece

European Conference on EDGE AI Technologies and Applications - EEAI

Edge-AI-IoT Standardization Activities

Erwin Schoitsch

AIT Austrian Institute of Technology, Austria

17-19 October 2023 Athens, Greece

Copyright © 2023

Introduction – AI4CSM & related Projects AIMS5.0, A-IQ Ready

Automotive Intelligence for Connected Shared Mobility

AIMS 5.0

Artificial Intelligence in Manufacturing leading to Sustainability and Industry5.0

AI using Quantum measured Information for Real-Time Distributed Systems at the Edge

Standardization Tasks focus on Artificial Intelligence - generic as well as domain-specific in all of these projects

Copyright © 2023

Joint Vision & Objectives of Standardization in European Projects

Joint Vision on the role and impact of Standards:

- Following the **European VISION** related to **Standardization**, supporting **Sustainability, Resilience & Digital Sovereignty as well as Ethical & Human Centred Aspects‘ (public acceptance) by addressing different domains, the “Green Deal” and the UN Sustainable Development Goals**.
- **Meeting the public stakeholders' interests** by addressing quality, safety, security, dependability, performance and ethical aligned design, human and environmental aspects, following European Recommendations, Directives and Regulations.
- **Enabler of a Fair and Competitive Economy** (through Interoperability and Provision of Common Requirements)
- **Enabler of a resilient economy and society** (exchangeable products and components → more resilient production and supply chains)

Joint Objectives of Standardization Tasks in Research Projects:

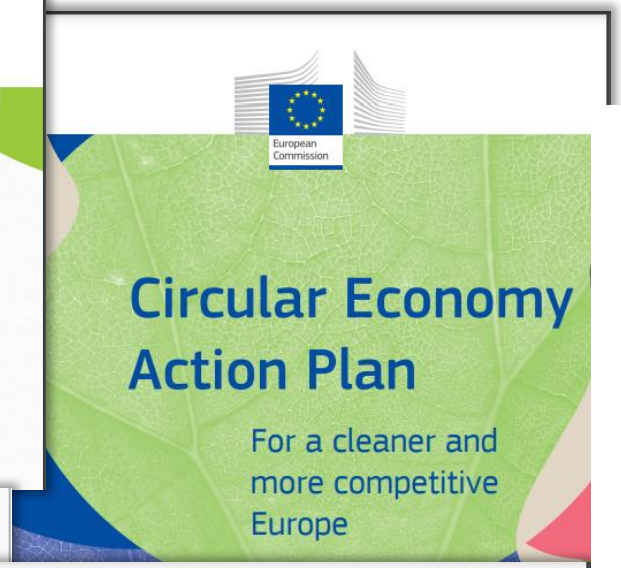
- **Raising awareness of partners on existing and evolving standards in their work (from “early adopters” to “users”).**
- **Support project partners in ensuring conformance of R&D work results with current and upcoming standards as well as influencing standardization** by driving new knowledge and experiences into the standards.
- **Analyze and evaluate AI Implementation, relevance of Ethical Aspects and “Human-in-the-Loop” issues, Trustworthiness and Ethical/Societal aspects** in context of project development and use cases.
- **Bring forward project concepts to standards – identifying “Windows of Opportunity”** (in “Artificial Intelligence”, “IoT & Digital Twin”, “Automated Driving”, “Smart Manufacturing”, “Cybersecurity Engineering” and “Functional Safety”).

Copyright © 2023

State-of-the-art – Ethical and Security Recommendations

Copyright © 2023

State of the Art - Targeting Sustainability, Resilience & Sovereignty



Require Standardization Frameworks & Harmonized Standards

Copyright © 2023

Research, Standardization & Development Goal - Trustworthiness

Definition: Trustworthiness Landscape – ISO/IEC JTC1 WG13

… **”ability to meet stakeholders’ expectations in a verifiable way”** (ISO/IEC TS 5723:2022 Trustworthiness— Vocabulary)

→ More than just functional safety, cybersecurity or performance, requires assessment of ALL stakeholders’ interests in context of a system or system of systems.

The following characteristics of Trustworthiness have been used to determine the activities of WG13:

Accountability, Accuracy, Authenticity, Availability, Controllability, Integrity, Privacy, Quality, Reliability, Resilience, Robustness, Safety, Security, Transparency, Usability,

→BUT depending on the stakeholders to take into account, it could also include public acceptance, financial and economic aspects, environmental or ethical issues etc.

« AI – Trustworthiness Standards

ISO/IEC TR 24028 - Overview of trustworthiness in AI
ISO/IEC TR 24029 - Assessment of the robustness of neural networks(Part 1 & 2 published, Part 3 under development)
ISO/IEC 23894 – AI – Risk management
ISO/IEC 25059 (SQuaRE) — Quality model for AI-based systems
ISO/IEC CD TR 5469 - Functional safety and AI systems
… and about a dozen others (published or under development)

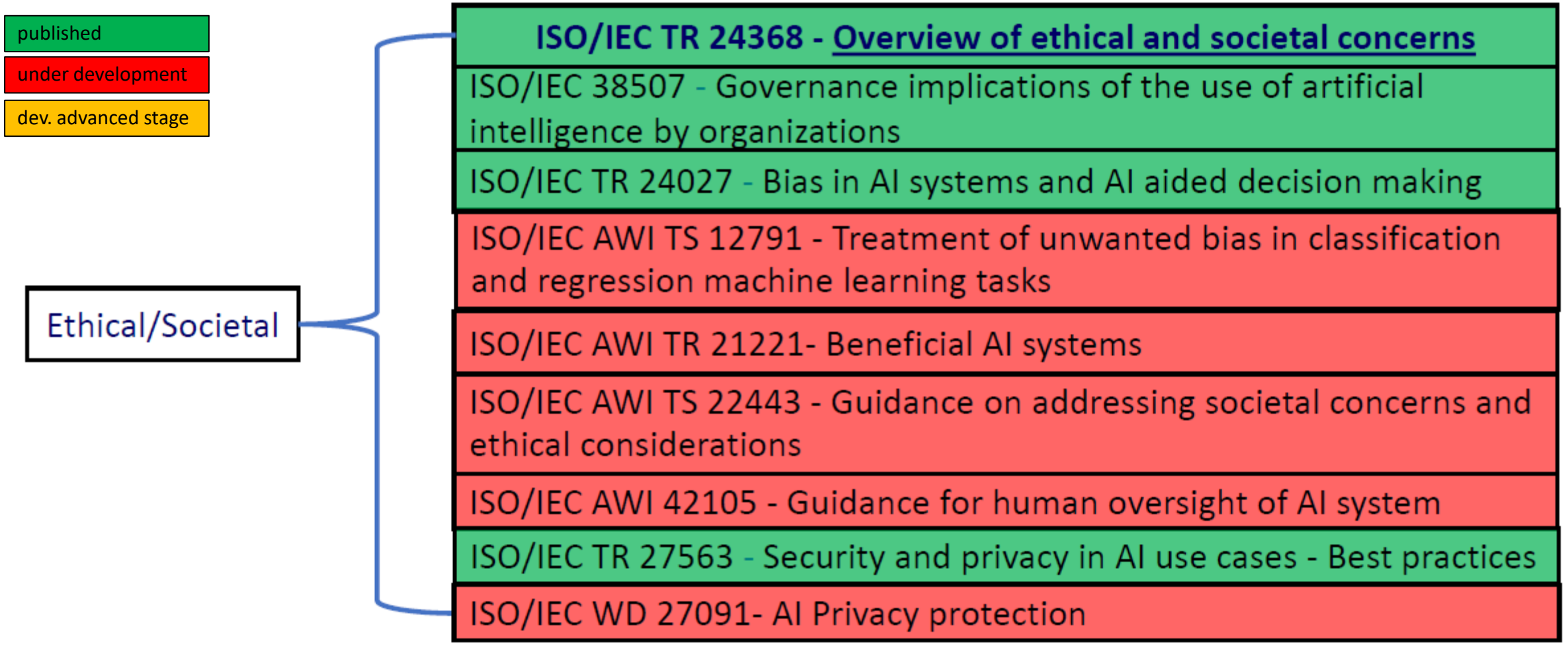
published
under development
dev. advanced stage

IoT – Trustworthiness Standards

ISO/IEC 30147 - (IoT) - Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes
ISO/IEC DTS 30149 – IoT – Trustworthiness principles
ISO/IEC 30187 ED1 IoT- Evaluation indicator for IoT systems

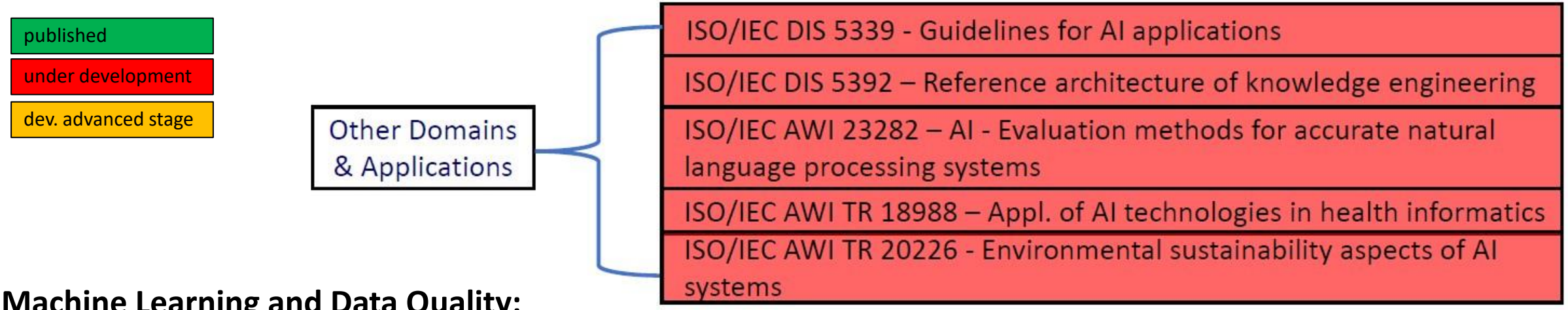
Copyright © 2023

AI Trustworthiness Standards – Ethical/Societal related



Copyright © 2023

AI Trustworthiness Standards – ML, Data, other Domains



Machine Learning and Data Quality:

- ISO/IEC CD 5259-X (under development) — AI - Data quality for analytics and machine learning (ML) (6 parts)
- ISO/IEC AWI TS 6254 (under development) — Objectives and approaches for explainability of ML models and AI systems
- ISO/IEC CD TR 17903 (under development) IT— AI— Overview of machine learning computing devices
- ISO/IEC AWI TR 42103 (under development) - IT— AI— Overview of synthetic data in the context of AI systems

Software Quality and Systems Engineering:

- ISO/IEC AWI TS 17847 (under development) – AI - Verification and validation analysis of AI systems
- ISO/IEC AWI TS 25058 (under development) - Software and systems engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guidance for quality evaluation of AI systems
- ISO/IEC AWI TS 29119-11 (under dev.) SW and systems engineering — SW testing — Part 11: Testing of AI systems
- ISO/IEC AWI TR 42106 (under development) AI— Overview of differentiated benchmarking of AI system quality characteristic

Copyright © 2023

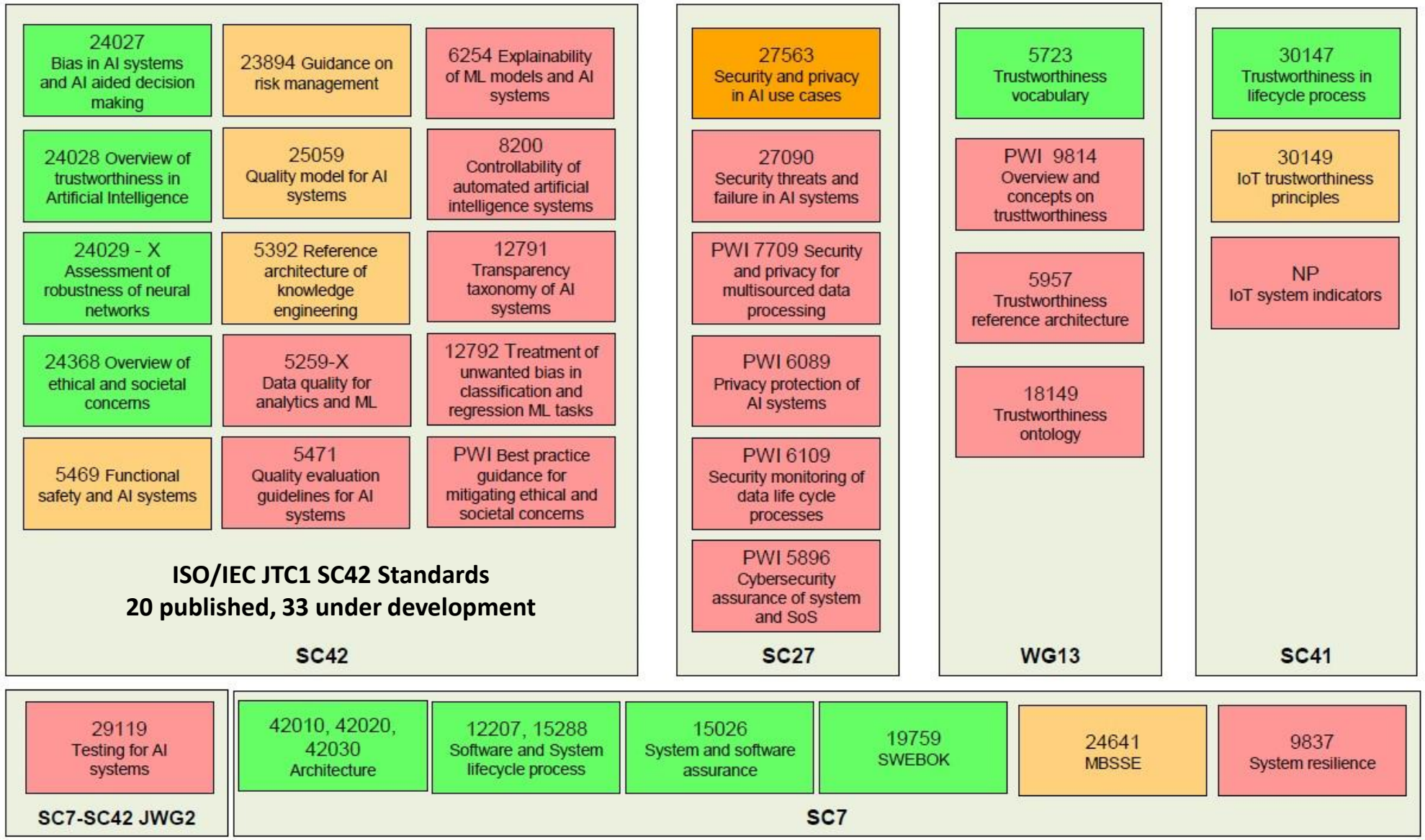
Trustworthiness Standards across ISO/IEC JTC1

Green = Published,
Orange = CD stage
Red = before CD

Subcommittees and WGs in ISO/IEC JTC1:

- **SC 7 Software & Systems engineering**
- **SC 27 Security and privacy**
- **SC 41 IoT and DigitalTwin**
- **SC42 AI**
- **WG 13 Trustworthiness**

Source:© ISO/IEC JTC1
AhG7, Antonio Kung

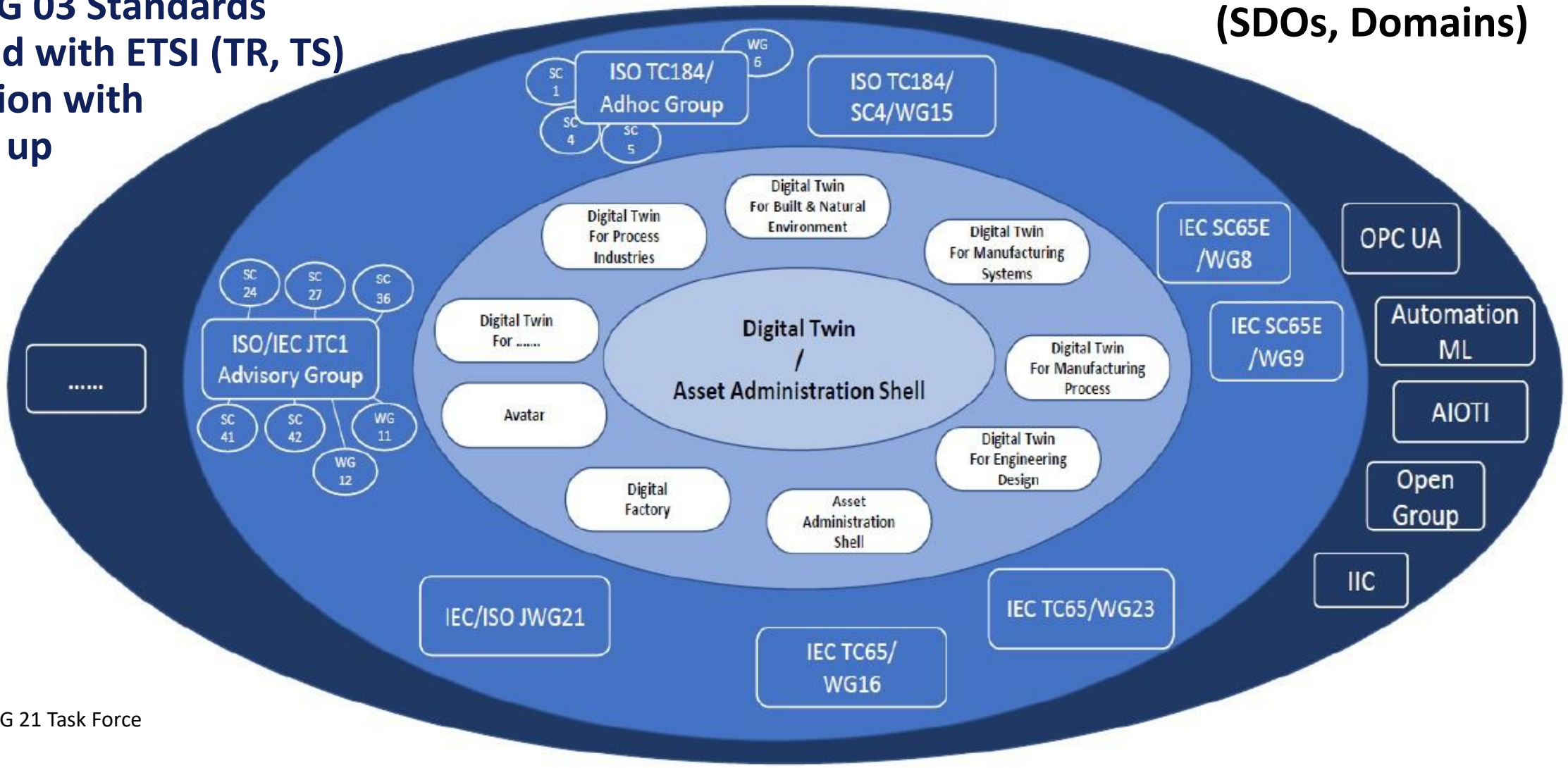


Copyright © 2023

AIOTI – Alliance for IoT and Edge Computing Innovation

- Publication of Reports,
- AIOTI WG 03 Standards published with ETSI (TR, TS)
- Connection with AI taken up

IoT – Digital Twin Eco-System (SDOs, Domains)



Source: IEC TC65 JWG 21 Task Force

Copyright © 2023

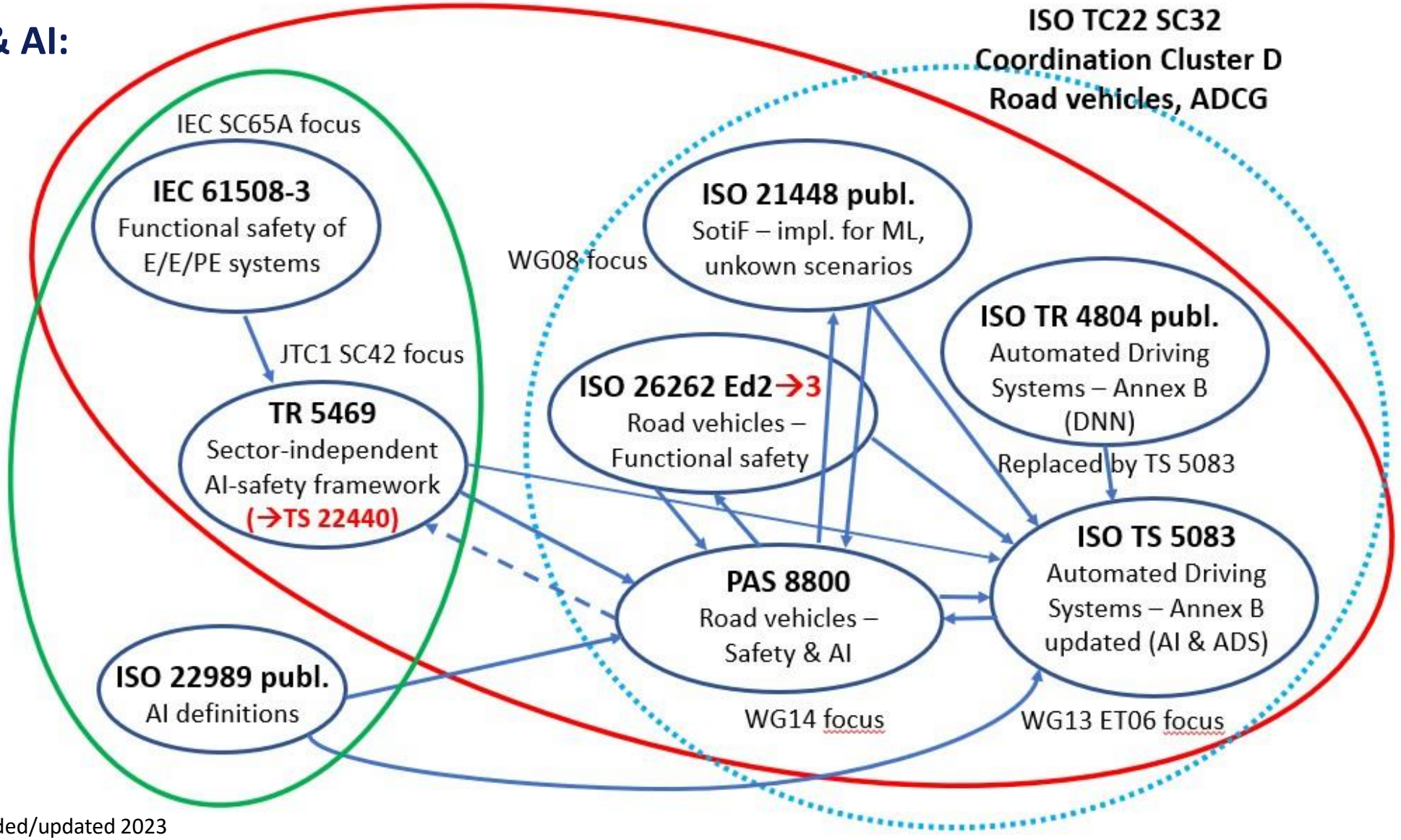
Methodology – Working in various Standardization Groups

Example Automotive & AI:

Across several

Committees and WGs

Note:
Red circle = Partners' active Involvement



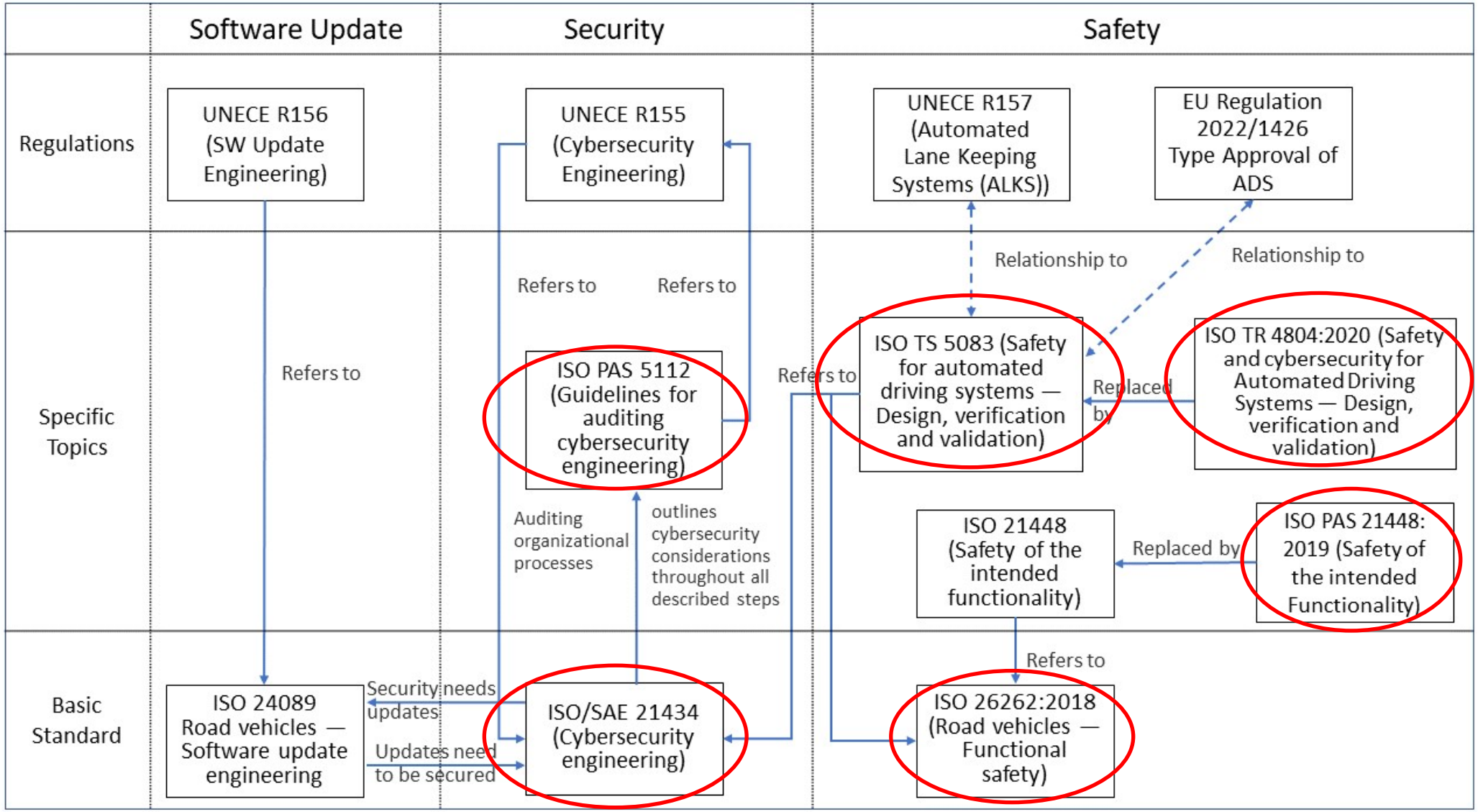
Source: ISO TC22 SC32 WG13 ST06, extended/updated 2023

Copyright © 2023

More than just Standards – Harmonized for Regulations

Automotive Example:
Regulations and related Standards

Partners' involvement (history)



Copyright © 2023

IEC TC65 WG 23, 24, JWG21 – Smart Manufacturing

- IEC TR 63283-1 ED1: Smart Manufacturing – Part 1: Terms and definitions
- IEC TR 63283-2 ED1 (under development): Smart Manufacturing – Part 2: Use cases
- IEC TR 63283-3 ED1: Smart Manufacturing – Part 3: **Challenges for Cybersecurity**
- IEC TR 63283(-4) WD (under development): Smart Manufacturing – Part 4: New technologies

  This document is a technology-oriented "Smart manufacturing trend analysis". The identified new technologies relevant are:

  - **AI**
  - **Edge computing;**
  - Cloud technology;
  - **Digital twin;**
  - New communication protocols, 5G, TSN;
  - Big data and data analytics;
  - **IoT and IIoT**;
  - Privacy technology, etc.

  Each chapter has a subchapter on "Technology description", "Use case analysis" and "Standardization needs".
- **IEC TR 63283-5 ED1** (under development): Smart Manufacturing – Part 5: Market and innovation trends analysis
  - Industrial IoT, (I)IoT devices, Edge, Cloud, 6G and AI are the key topics and sections,

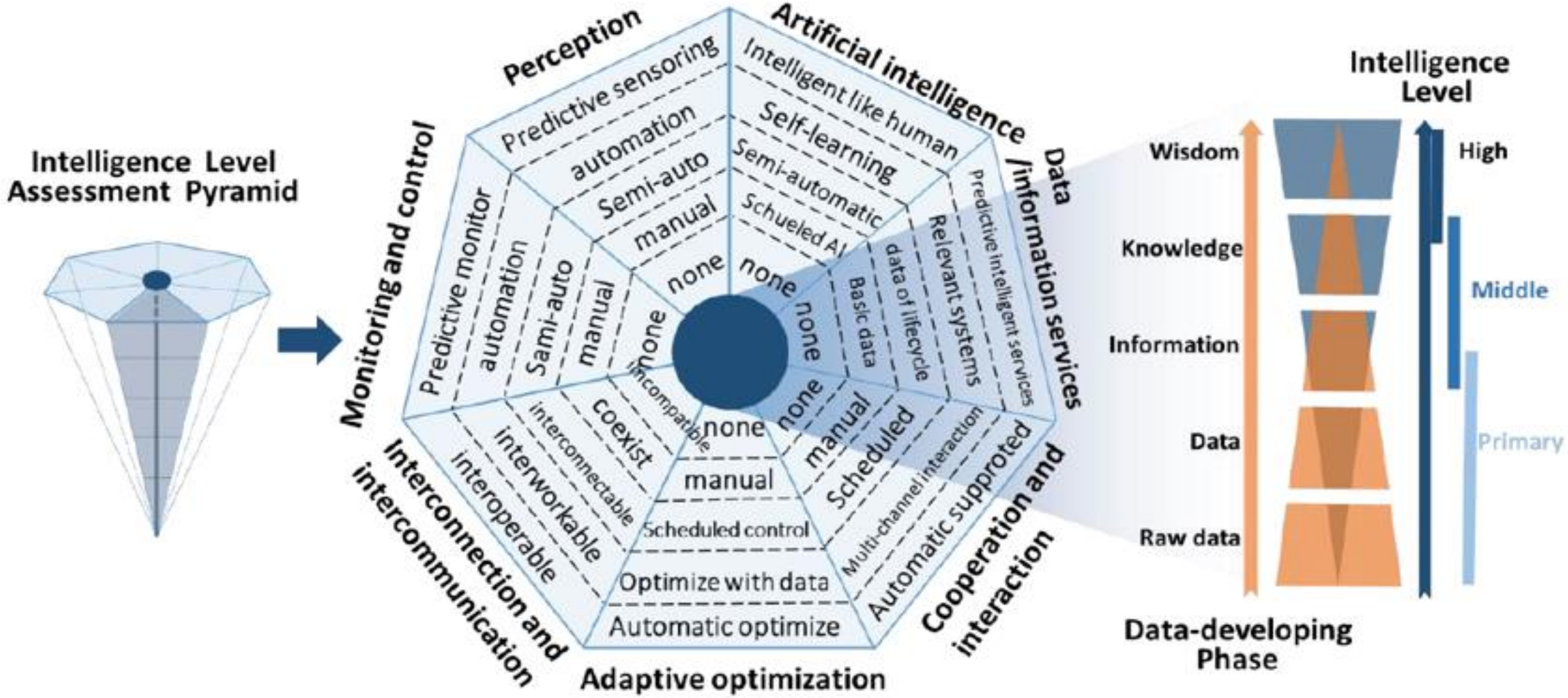
Further ideas handled by TFs:

- *IEC TR 63283-6 ED1 (CD under development): Evaluation of intelligence properties for SM*
- *IEC TR 63283-7 ED1 (draft under development (DE NC)): SM recommendations for safety*
- *IEC TR 63283-8 ED1 (TF started, collecting requirements): SM Gap Analysis*

Copyright © 2023

IEC TC65 WG 23, 24, JWG21 – Smart Manufacturing

IEC TR 63283-6 ED1 – Evaluation of Intelligence Properties & Assessment



Copyright © 2023

Trust - Critical Challenge: Functional Safety and AI Systems – ISO/IEC DTR 5469

AI Technology Classes:

- **Class I:** AI technology can be developed and reviewed using existing methods & standards
- **Class II: Not fully Class I, but** still possible to identify a set of available methods and techniques satisfying the safety properties
- **Class III: Cannot** be developed and reviewed using ex. methods & standards and no available methods & techniques satisfying safety prop.

Usage Levels:

- **A1: AI** used safety relevant & automatic decision
- **A2: AI** used as in A1, but NO automatic decision
- **B1: AI** used during development **(offline support tool)** & automated decision making
- **B2: AI** used as in B1, but NO automated decision
- **C: AI** not part of a safety function, but can have impact on safety (e.g., increasing demand rate)
- **D: AI** is not part of a safety function, no impact on safety (segregation, behavior control)

Further: Very detailed analysis of:

- **Risk factors and mitigation, processes&methodologies**
- **Verification and Validation (AI specific challenges)**
- **Data preparation and model-level V&V, etc.**

<table>
<tr><th>AI Technology Class => AI application and usage level</th><th>AI technology Class I</th><th>AI technology Class II</th><th>AI technology Class III</th></tr>
<tr><td>Usage Level A1 (1)</td><td rowspan="5">Application of risk reduction concepts of existing functional safety International Standards possible</td><td>Appropriate set of requirements (5)</td><td rowspan="5">Not recommended</td></tr>
<tr><td>Usage Level A2 (1)</td><td>Appropriate set of requirements (5)</td></tr>
<tr><td>Usage Level B1 (1)</td><td>Appropriate set of requirements (5)</td></tr>
<tr><td>Usage Level B2 (1)</td><td>Appropriate set of requirements (5)</td></tr>
<tr><td>Usage Level C (1,3)</td><td>Appropriate set of requirements (5)</td></tr>
<tr><td>Usage Level D (2)</td><td colspan="3">No specific functional safety requirements for AI technology, but application of risk reduction concepts of existing functional safety International Standards (4)</td></tr>
<tr><td colspan="4">1 Static (offline) (during development) teaching or learning only
2 Dynamic (online) teaching or learning possible
3 AI techniques clearly providing additional risk reduction and whose failure is not critical to the level of acceptable risk.
4 Additionally, other safety aspects (not being addressed with functional safety methods) can possibly be adversely affected by AI usage.
5 The appropriate set of requirements for each usage level can be established in consideration of Clauses 8, 9, 10 and 11. Examples are provided in Annex B.</td></tr>
</table>

Copyright © 2023

Conclusion

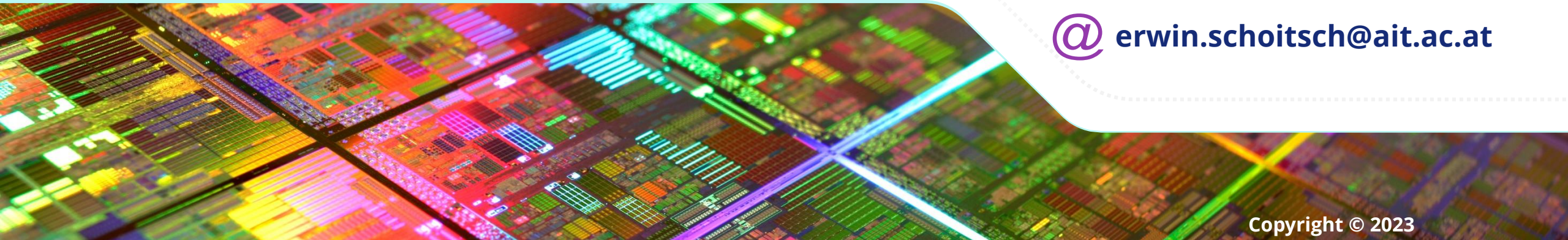
- The large landscape of standards in AI/IoT/Trustworthiness generic as well as specific for domains opens many **“windows of opportunity”** to contribute/influence standards, i.e., that results and experiences from research projects (technology development and use cases/demonstrators) can be brought forward and exploited in standardization work.
- The currently **collaborating projects (EEAI Cluster) allow for synergies** in work and standardization, building on sequences of related projects, of past and current results/experiences exchanged during collaboration.
- Standardization work is in most cases lasting longer than Horizon research projects, they need **long term commitment** of key partners – this is guaranteed in practice by the model of Horizon project partners to work in a longer series of projects together.
- There have been already **achievements** reported in several projects wrt. standardization: A key element was that issues like avoidance of unnecessary parallel work on related topic could be achieved by collaboration of different groups and strengthening links, like
  - IEC 61508-3 and ISO/IEC JTC1 SC42 WG03 on Functional safety and AI, based on industrial and research experience; or in
  - Automotive between related groups as indicated in the slides, promoted by partners; or
  - Cybersecurity engineering in Automotive, and linking Functional safety standards with cybersecurity challenges.
  - Supporting new work item “Human Oversight”.
  - Enabling new important standardization work items (NWIP) by motivating additional NCs (National Committees) to delegate experts (examples: Predictive maintenance in IACS, Cybersecurity in SM, OO SW in Functional safety).
  - in the past including time-triggered protocols in IEC 61508-3 and 61508-7 (DECOS-project in FP7).
- **Let’s Go ON!! Be Involved!!**

Copyright © 2023

EDGE AI

Thank You

For your attention



@ erwin.schoitsch@ait.ac.at

Copyright © 2023