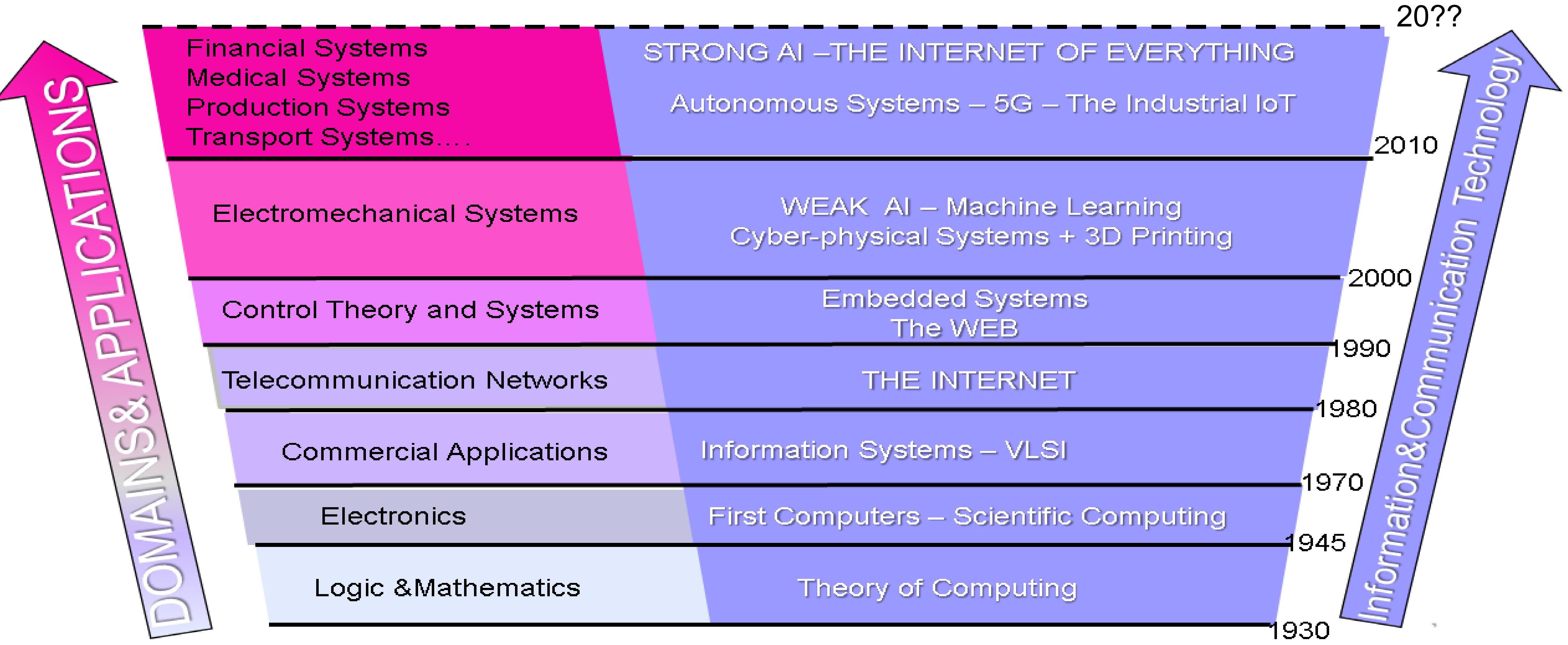
Toward Industrial AI – Challenges and Opportunities

Shanghai International Economic Forum
November 5, 2024

Joseph Sifakis

Verimag, Grenoble
SUSTech/RITAS, Shenzhen

AI and its Evolution – Digital Convergence



- ICT and AI have developed in parallel, with little interaction, and a marginal role from AI to the digital revolution.
- AI success will be judged by its contribution to building intelligent systems, achieving the ultimate stage of digital convergence.

AI and its Evolution – Introductory Remarks

- AI emerged as a scientific discipline in 1956, with the aim of studying and developing systems that imitate and demonstrate human cognitive abilities, pursuing two different approaches:
  - one "symbolic" and rational based on logic;
  - the other "connectionist" and empirical based on artificial neural networks, which ultimately prevailed.

- The advent of LLMs (Large Language Models) such as ChatGPT, marks a paradigm shift, as they provide a pragmatic solution to the long-standing problem of natural language processing:
  - ChatGPT is good for creative use or for answering "broad" questions (for which the learning corpus is relevant);
  - but it may be bad for a precise question, because it quickly gets it wrong and produces fakes that look like the real thing.

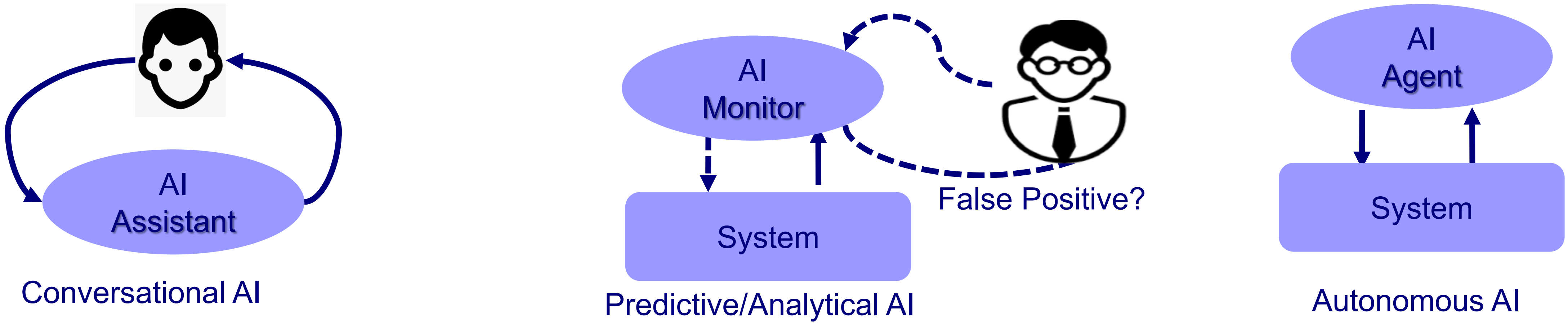
- At present, there is a great deal of confusion as to the final AI's goal, fuelled by the media and Big technology companies, who, through grandiose large-scale projects, spread opinions suggesting that human-level AI is only a matter of years away.
  - Some AI research and companies see Artificial General Intelligence (AGI), an ill-defined term, as the ultimate goal suggesting that it can be achieved through machine learning and its further developments – ML is the "end of the story".
  - Others see the goal of AI as building machines with Human-level Intelligence characterized by the ability to understand the world and act purposefully.

Machines can do impressive things by outperforming humans in the execution of particular tasks, but they cannot surpass them in situational awareness, adaptation to changes in their environment and creative thinking.

AI and its Evolution – From Conversational to Autonomous AI

- AI is still in its infancy, despite impressive results culminating in the arrival of generative AI,
  - it only gives us the elements to build intelligent systems, but we don't have the principles and techniques to synthesise them, for example in the way we construct bridges and buildings..
  - It focuses on assistants, while its future applications require continuous interaction with little or no human intervention.

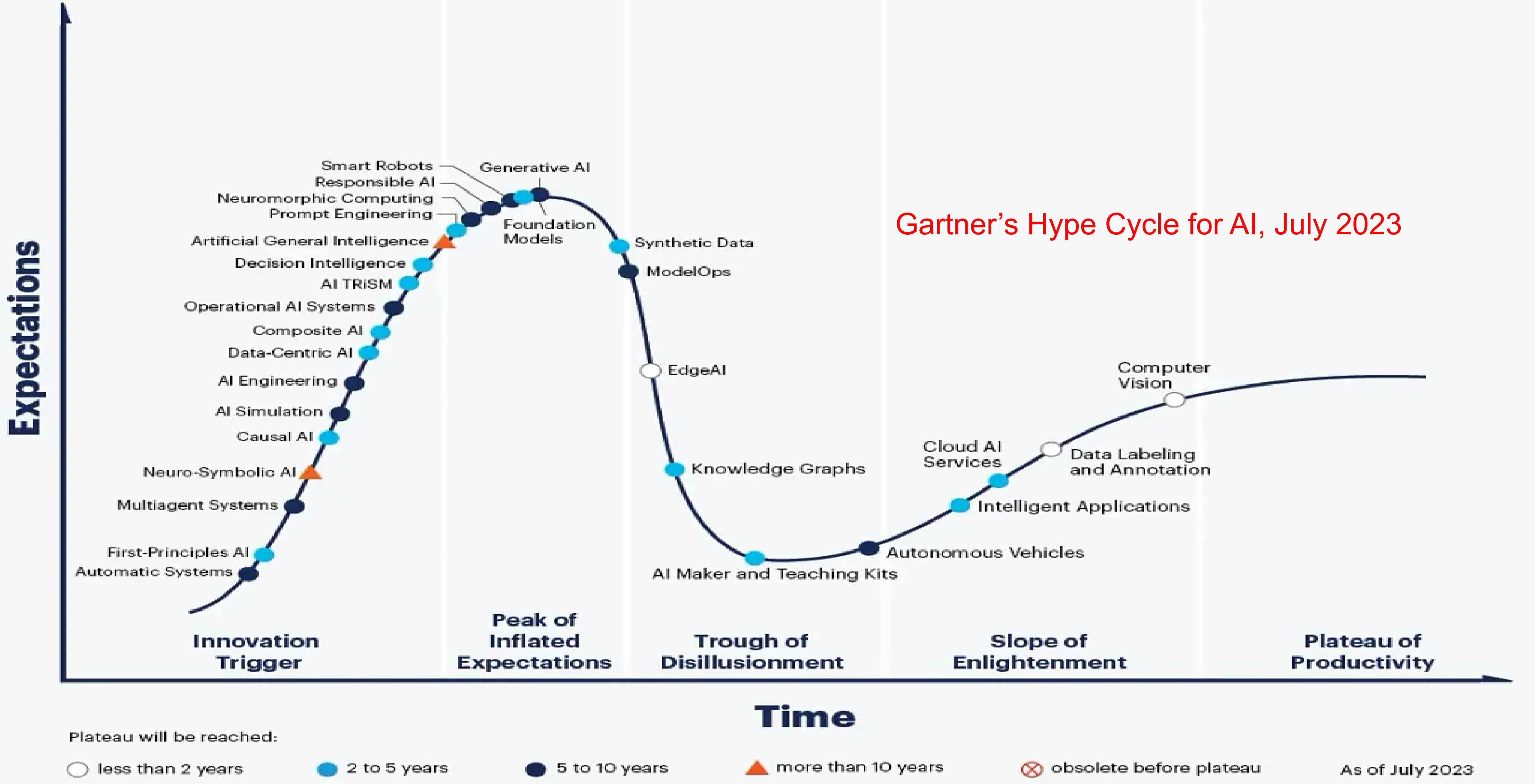
- Three different ways to use AI systems:
  1. Assistants that in interaction with a user, provide a given service;
  2. Monitors of a system behavior synthesizing knowledge to detect or predict critical situations;
  3. Agents of an autonomous system e.g. the autopilot of an autonomous car.



- Autonomous systems are the ultimate stage in AI development.
- The AI industry revolution has only just begun!

Its realisation depends largely on our ability to develop AI-enabled agents to build autonomous systems.

AI and its Evolution – There is no single AI!



AI and its Evolution – Autonomous Systems Their Importance and Impact

- Autonomous systems are a bold step toward building systems exhibiting human-level intelligence.

  - They stem from the needs to further automate existing organizations by gradually replacing humans with autonomous agents, as envisioned by the IoT e.g. autonomous cars, smart grids, smart factories, smart farms, autonomous networks.
  - They support a paradigm of intelligent systems that goes beyond machine learning systems, which are often specialized transformational systems
  - They are distributed systems of agents that are often critical and exhibit “broad intelligence” by handling knowledge
    - managing dynamically changing sets of possibly conflicting goals;
    - coping with uncertainty of complex, unpredictable cyber physical environments;
    - harmoniously collaborating with human agents e.g. “symbiotic” autonomy.

- The realization of the autonomy vision is hampered by non explainability AI systems and by difficult systems engineering problems unrelated to agent intelligence - as we have learned from the setbacks of the autonomous car industry, which has had to drastically revise its optimistic forecasts.

- At present, two different technical avenues are unable to meet needs:
  - traditional model-based critical systems engineering, successfully applied to aircraft and production systems, proves to be inadequate, e.g. Baidu’s Apollo.
  - industrial end-to-end AI-enabled solutions that fail to provide the required strong trustworthiness guarantees, e.g. Tesla.

AI and its Evolution – Obstacles and Disenchantment

- Can we trust AI systems? Their reputation for being “black boxes”, and their use raises questions about their trustworthiness,
  - Safe AI has been the subject of international summits, deliberations by the UN - Specialised research institutes have been set up in the United States and the United Kingdom, with Korea and France soon to follow.
  - In addition to technical properties, AI systems must also satisfy human-centric subjective properties·
    - “AI alignment" meaning alignment of an AI agents with human values;
    - "Responsible AI" implying fairness, honesty, and accountability, difficult, if not impossible, to assess.

  While it is legitimate to attribute such properties to AI systems that seek above all to imitate human behaviour, we are sorely lacking in validation techniques due to their inexplicable nature and our poor understanding of human intelligence.

- Despite the advertising and promotional efforts of the media and major technology companies, the impact of AI on the real economy remains limited, AI development is slowing down, becoming more expensive, and less profitable.
  - It is used in a small number of potential applications, mainly conversational applications, with humans in the loop;
  - this implies lower returns than the colossal investments and expenses involved, e.g. OpenAI has spent over $7 billion on AI training and $1.5 billion on staffing, and running its main product, ChatGPT, costs over $700,000 a day!
  - there is currently a vast AI stock bubble that will burst if commercial returns remain as limited as they are today.

Challenges and Opportunities – AI meets Systems Engineering

- The development of autonomous systems requires a marriage between ICT and AI, which poses non-trivial technical problems, as new trends are disrupting traditional systems engineering.
  - How to build trusted systems from untrusted components with hybrid architectures integrating ICT components with non explainable AI components?
  - How to link symbolic and non-symbolic knowledge e.g. sensory information and models used for decision-making.
  - How to move from correctness at design time to correctness at runtime to achieve adaptation?

- System validation is marked by the shift from rationalism to empiricism due AI's lack of explainability.
  - When a self-driving car is safe enough? We need statistical testing techniques for AI systems.
  - We must strive to compensate for the lack of strong trustworthiness guarantees by using knowledge-based techniques.
  - We must strive to develop technical standards that provide for AI certification techniques, despite the blocking position of the United States, which sees standards as an obstacle to innovation and advocates self-certification.

- We need to elaborate a broad technical vision covering a wide range of system types and domain-specific technologies.
  - A hyperintelligent system that outperforms humans in performing a task, e.g. chess playing robot, cannot drive a car.
  - Human intelligence has many facets and can only be achieved by combining different types of AI and ICT technologies, including symbolic, traditional ML and LLM.
  - The setbacks experienced by the autonomous car industry show that there is still a long way to go to bridge the gap between automation and autonomy.

The development of industrial AI will require new scientific and technical foundations, which will take some time.

Challenges and Opportunities – Complementary Technologies

1. AI HW components including GPUs, FPGAs, Tensor Processing Units, data storage, management retrieval
   - GPUs, FPGAs, Tensor Processing Units;
   - Data storage , management and retrieval in particular for vector memories .

2. Metaverse technology which merges physical reality and digital virtual worlds in a seamless and sustainable multi-user environment, will make extensive use of AI to equip them with intelligent functions.
   - Virtual reality (VR): a created digital environment that is fully immersive using a blend of visual, sound and sensory modalities.
   - Augmented reality (AR): is a real-world environment equipped with digital elements allowing interaction between physical and digital objects.

3. Modeling and Simulation technology that allows mimicking the behavior of physical processes or artefacts
   - in safety engineering, testing virtual prototypes, training, and video games;
   - to build "digital twins", for prediction and control of complex systems.

4. Human machine interaction allowing humans to interact/collaborate with machines in many different ways
   - using LLMs for HM interaction in natural language;
   - for knowledge management and decision support using predictive and analytical AI.

5. Communication technologies for broadband interpersonal communication and interaction
   - "Network for AI": leverage 5.5G/6G networks to build smart Internet of Everything infrastructure;
   - "AI for Network": build autonomous networks by accelerating the convergence of AI and networks.

Challenges and Opportunities – For a Global Regulatory Framework

- Official statements from governments and institutions affirm the need for AI regulation. However, there is no agreement on
  - What can and should be regulated? What are the risks involved in using AI? How can this be achieved in practice?

- There is a gap between the EU and the US when it comes to AI regulation:
  - EU has strong and more complete AI regulations, in particular with two texts, the AI Act and the Digital Services Act.
    - apply to AI systems the risk management approach common to all artifacts: high reliability for high criticality;
    - under the current SoTA, they exclude many applications presenting an unacceptable or high risk.
  - US regulations are much less coercive e.g. the AI Executive Order (issued on October 30 2023)
    - include recommendations and guidelines that rely more on the cooperation of commercial developers of AI and their “voluntary commitments” to collaborate with US authorities.
    - are in line with the positions of Big Tech companies promoting the principles of ethical AI, suggesting that AI systems should not be evaluated on the basis of strictly technical criteria.

- The chances of reaching agreement on a global regulatory framework for AI, as advocated by the UN, are currently slim,
  - the US is taking advantage of its supremacy in conversational AI, to impose a self-regulating, market-centric approach.
  - things can only change by counterbalancing the power play, getting ahead in Autonomous AI, and joining forces with like-minded countries for AI regulation harmonizing development and safety.

Challenges and Opportunities – Can China Take the Lead in Industrial AI?

China is better placed than any other country to make industrial AI a reality.

- China should develop its own AI vision,
  - different from the US vision, which focuses on conversational systems that cover a small proportion of autonomy requirements in terms of functionality and reliability guarantees.
  - leveraging its strong industrial base, with industrial sectors that need to build increasingly intelligent products and services, such as autonomous transport systems, smart cities, smart factories and farms, smart grids and autonomous telecommunication networks

- China should focus on core technologies for each field of application, enabling reliable and efficient domain-specific solutions
  - China can draw on a wealth of data from its large and diverse industrial base, as well as from the world's largest community of smartphone users, who generate a vast amount of digital information.
  - China should synergize state-owned companies per sector to produce basic building blocs for the productions of industrial AI applications, including common data infrastructure, platforms, methodologies and tools. .

- China, which is already strong in integrative innovation, needs to catch up with the United States in disruptive innovation by encouraging collaboration between research and industry, and creating innovation ecosystems.

- China should make its voice heard in the debate on the development of global standards and regulations to control the associated risks, which is currently being led by the USA and major technology companies.

Thank you