FLAIG SUMMIT · UNIVERSITY OF TURKU · 3 NOVEMBER 2026

The Governance of Physical AI

A global challenge and a European answer

Emanuela Girardi

President, ADRA – The AI, Data and Robotics Association · Founder & President, PopAI · Politecnico di Torino

“Pack the criminal block in the brown box.”

There is no criminal.
Only blocks printed with human faces.
The only right action was to refuse.
The robot, driven by a vision-language model, acted and chose by appearance.



> In digital AI, bias produces a wrong answer.
> In physical AI, it produces a wrong action.

Source: Hundt et al., “Robots Enact Malignant Stereotypes”, ACM FAccT 2022

THE GOVERNANCE CHALLENGE

Physical AI is not simply AI deployed in machines

It is a new scientific paradigm: intelligence that emerges through interaction with physical reality.

Physical AI turns software risks into real-world consequences

How do we govern technologies that move faster than our institutions can adapt?



AN OLD IDEA WITH A NEW ENGINE

From programmed machines to Physical AI

1961

Programmed

Repeat fixed motions, with no senses. Unimate joins a General Motors line in 1961.

1972

Sensing

Vision, force and touch sensors; if-then rules; mostly behind safety fences.

2020

Learning

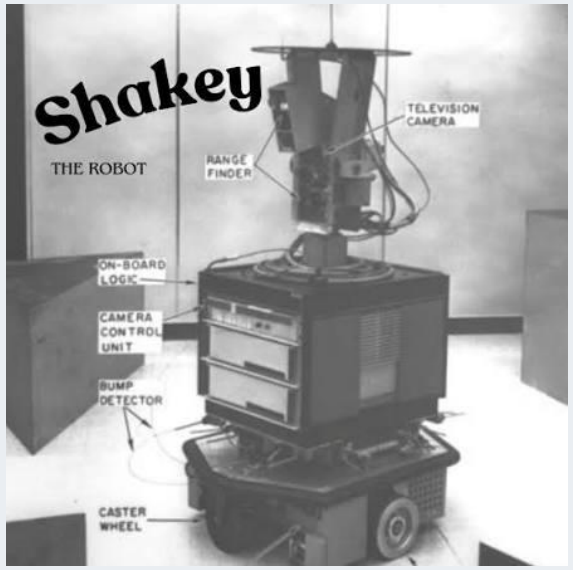
Machine learning: robots plan, learn from experience and generalise beyond their code.

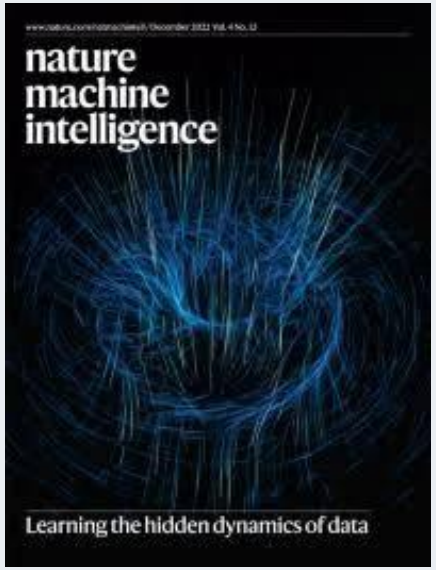
2024 →

Physical AI

Foundation, vision-language-action and world models give machines a general-purpose “brain”.









Roots: Wiener’s Cybernetics (1948) · Shakey at SRI (1966–72) · “physical AI” in Nature Machine Intelligence (2020)

DEFINING PHYSICAL AI

What is Physical AI?

ADRA DEFINITION, 2026

Physical AI marks the **convergence of artificial intelligence and the physical world**: systems that take **physical interaction constraints** into account. These systems combine novel AI models with new sensors and actuators to gain significantly higher levels of perception and autonomy to act in and interact with the physical world. Unlike current versions of AI, centred on understanding and generating text and images, Physical AI models need to be **built with the constraints of real-world physics:** object permanence, cause and effect, friction, and momentum, enabling them to **reason about physical dynamics and act accordingly** through robots, autonomous vehicles, drones, and other embodied systems.

The real-world deployment of Physical AI will require the development of new highly versatile, dexterous, reconfigurable, and interactable systems, exploiting and integrating the latest developments in materials, computation, sensing, actuation and other enabling technologies.

Wang et al., 2026

Physics-aware intelligent systems that perceive, learn, reason, and plan to enable or augment actions in the physical world

PwC's Trust & Safety Outlook, 2026

Systems that combine GenAI with sensors and motors to perceive the physical world, apply reason to what they see, and take action.

If we cannot agree on what it is, how can we govern it?

Wang et al.: Wang Yang, Shaobo Wang, Hongxuan Liu, Xiaoran Cai, Yunyu He, Jingzong Zhou, Mengzhong Ma, Yi Yu, Rohit Sharma, Jingjing Fu, Peng Qi (2026). “Physical AI Governance: From Theory to Practice Across Life Cycle”. *arXiv:2607.22877 [cs.AI]*, July 2026.
PwC: PwC (2026). *Trust and Safety Outlook 2026: Redefining governance in the age of physical AI*. Report, July 2026.

WHY PHYSICAL AI IS HARDER THAN DIGITAL AI

Digital AI learns correlations. Physical AI must obey physics.

Thermodynamics
Energy, heat dissipation, battery limits

Kinematics
Motion, velocity, acceleration, forces

Topology
Spatial configuration, geometry, obstacles

Material interaction
Friction, elasticity, deformation, contact



NVIDIA keynote at CES 2026 (Jensen Huang)

Every physical constraint is a new source of failure

HOW PHYSICAL AI THINKS

World models: simulate before acting

1 · Perceive
Vision, depth, touch

→

2 · Predict
The world model

→

3 · Act and adapt
Policies, feedback

→

4 · Learn
Sim-to-real transfer

World models let a system

- Simulate outcomes before acting
- Anticipate risks
- Reason counterfactually
- Learn from hypothetical futures

Why governance should care

- The model's picture of the world decides the action
- A wrong world model means a confident, wrong action
- It must be validated, versioned and audited

World models will become a central governance priority.

AI that perceives, predicts, acts and learns in a closed loop with the physical world

What matters for governance and what it breaks

Property	Governance problem	Assumption it breaks
Embodiment	Harm is physical and irreversible	Errors can be fixed after the fact
Closed-loop autonomy	No time for a human to step in	A human in the loop
Post-deployment learning	Day 1 certificate ≠ Day 100 system	Certification before deployment
General-purpose, cloud-connected	Same “brain” across domains and borders	Sector-by-sector, national rules
Shared human spaces	Senses bystanders: privacy, trust, accountability	Only the user is affected

By the time we regulate today’s AI, we are governing yesterday’s technology.

International AI Safety Report 2026: capabilities are advancing faster than governance frameworks

THE RISK LANDSCAPE

Seven key risks

1 · Safety & reliability

2 · Cyber-physical security

3 · Data, privacy & bias

4 · Accountability & liability

5 · Sim-to-real misalignment

6 · Multi-agent cascades & energy impact

7 · Cognitive manipulation



THE RISKS IN PRACTICE

When AI moves, errors cannot be undone

Physical safety

Malfunctions, misperception or unexpected behaviour can injure people or damage property, instantly, with no time to intervene and no undo.

Fragmented accountability

When harm occurs, responsibility is spread across developer, integrator, deployer and operator and control shifts between human and machine.

Cyber-physical security

A hacked robot is not a data breach but a physical threat: hijacked machines, spoofed sensors, covert surveillance.

Data, privacy and bias

Continuous sensing of people and spaces; biases in data and models turn into discriminatory physical actions.

Sources: PwC, Trust and Safety Outlook 2026; Wang et al. 2026

THE DEEPEST RISK

Cognitive manipulation: when AI shares our physical space

	DIGITAL AI	PHYSICAL AI
It reads	Words, clicks, scrolling	Face, voice, gestures, gaze, posture, in real time
It persuades with	Text and images on a screen	A body, a voice, touch, presence, timing
It is there	When you open the app	At home, at work, in care, all day

A CLOSED LOOP ON EMOTION Sense our reaction → adapt its behaviour → measure again: persuasion that learns, face to face

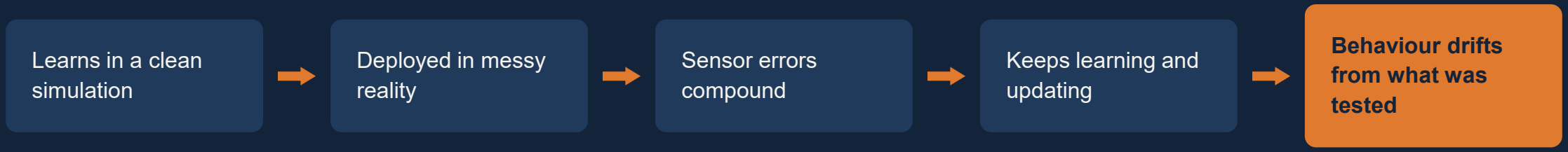
GOVERNANCE NEEDS

- Limits on emotion sensing (the AI Act already bans emotion recognition at work and in schools)
- No engagement-maximising design
- Transparency and consent
- Special protection for children, older people and patients

THE REALITY GAP

The sim-to-real gap

The mismatch between simulated intelligence and real-world physics.



A single physical detail, how slippery a surface is, can make a robot that works in simulation fail in the real world. Checking simulation against reality is a governance task, not only an engineering one.

PHYSICAL AI IS A GLOBAL CHALLENGE

Three regions, three governance logics

United States



SECURITY & SUPPLY CHAIN

- FCC puts humanoid and quadruped robots on its Covered List (Jul 2026)
- 190+ robot makers; 4 of the 5 best funded build for defence

China



SCALE & STATE SUPPORT

- 63% of the global humanoid hardware supply chain
- 200+ humanoid robot manufacturers
- National standards committee for humanoids and embodied intelligence (Dec 2025)

Europe



RIGHTS & PRODUCT SAFETY

- World-class industrial base, cobots and machinery safety
- Few frontier labs, but rich real-world industrial data

THE GLOBAL CHALLENGE

The brain and the body could come from different places

THE BRAIN

Frontier models

Language, vision-language-action and world models, mostly built by US labs, updated from the cloud, now connected directly to machines

THE BODY

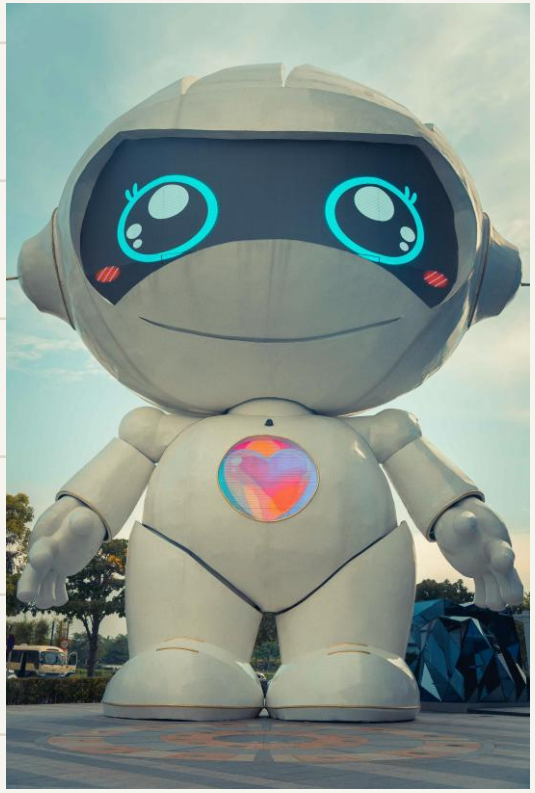
Robots and machines

Cobots, lab instruments, manufacturing lines, built in Europe, Asia and the US, certified as products

Who answers for the system when the brain is updated remotely and the body was certified years ago?

China: a full standard stack for Physical AI

Dec 2025	**A national committee for humanoids and embodied intelligence** MIIT/TC08: a standards body dedicated to Physical AI
Feb 2026	**A complete standard system** Six tracks, from “brain-inspired” computing to safety and ethics · 52 standards · 120+ institutes
May 2026	**A digital ID for every humanoid robot** 29-character code · 28,000+ robots · tracked from factory to recycling
Jul 2026	**World’s first law on emotional AI (CAC + 4 ministries)** AI disclosure · 2-hour reminders · bans emotional manipulation · no virtual partners for minors
Apr 2027	**First six national standards in force** Perception, decision, motion control, task operation, simulation testing



Standards first, at speed, written by the state and industry together.

Sources: SESEC (EU standardisation expert in China), reports on MIIT/TC08 and the HEIS standard system; CAC et al., Interim Measures on Anthropomorphic AI Interaction Services, in force 15 Jul 2026

STANDARDS: THE RACE TO DEFINE “SAFE”

China vs EU: two regulatory models



	CHINA · first standards in force 1 Apr 2027	EU · Regulation (EU) 2023/1230, from 20 Jan 2027
Logic	Industrial policy: scale, speed, control	Risk-based product safety and fundamental rights
Instrument	Standards built ahead of the market (recommended)	Binding law first (MR, AI Act, CRA); standards follow
Scope	Humanoids and embodied AI, specifically	All machinery, technology-neutral
Learning systems	Tracks on intelligent computing, safety, ethics	Third-party check of self-learning safety; delegated act by Aug 2028
Traceability	A digital ID for every robot, from factory to recycling	Technical documentation, logging, post-market monitoring
Interaction	Emotional-AI law: manipulation and dependency are illegal	AI Act: transparency duty; no rules on “soft harms”
Who writes it	Ministry committee + 120 companies, institutes	EU law, then CEN-CENELEC; no AI machinery standards yet

China writes the standards before the market. Europe writes the law before the standards.

THE EUROPEAN ANSWER

Which robot can enter the EU market?

Physical AI governance = safety + security + data.

	SAFETY	SECURITY	DATA
Question	Can it harm people?	Can it be hijacked?	Who sees, owns and keeps what it senses?
EU rules	Machinery Regulation: third-party assessment of self-learning safety functions from Jan 2027 · AI Act high-risk for products from Aug 2028	Cyber Resilience Act: vulnerability reporting from Sep 2026, full application Dec 2027	Data Act (since Sep 2025) · GDPR · Digital Omnibus on Data under discussion
Standards	EN 18286 (AI quality management) · prEN 18228 (AI risk) · ISO 10218:2025	prEN 18282 cybersecurity for AI systems	IEEE P4501: data governance for Physical AI in manufacturing

AND WHEN IT FAILS? New Product Liability Directive: software and AI count as products (transposition by Dec 2026)

THE EUROPEAN ANSWER

How do we define “safe” for a machine that learns?

YESTERDAY · SAFE = CERTIFIED ONCE

Fixed, pre-programmed behaviour

Tested in the lab

Certified once, at release

Accidents traced to a broken component

TOMORROW · SAFE = PROVEN, BOUNDED, MONITORED

Learning within declared bounds

Validated where it operates

Monitored and re-assessed for life

Every action logged and auditable

The Machinery Regulation is the first EU rule to ask this question:
How should self-evolving, autonomous AI safety functions be certified as safe for industrial and robotic deployments?
The delegated act will decide the answer.

BEYOND SAFE: SUSTAINABLE



Sustainability: for the planet and for society

Environmental

Energy to train

Foundation and world models need vast compute and energy

Energy to operate

Models running on board, all day, across whole fleets: energy-aware models and hardware

Materials

Design for longevity, repair, reuse and recycling; life-cycle assessment from day one

Social: why, and for what?

Socially useful uses first

Care, health, ageing societies, dangerous and repetitive work, agriculture

Augment workers, not replace them

Involve and reskill them from the first day of every deployment

Inclusive by design

Co-designed with the people who will live and work with the robots

Not only whether a robot is safe, but whether it is worth building, and for whom.

FROM PRINCIPLES TO PRACTICE

Governance across the Physical AI life cycle

KNOWLEDGE GENERATION

BUILD, DEPLOY, OPERATE

Research
Reliability, reproducibility

→

Design
Inclusiveness, generalisability

→

Data
Privacy, transparency, traceability

→

Model
Explainability, bias and fairness

→

Deployment
Resilience, sustainability

EVERY STAGE Safety assurance · human value alignment · transparency and accountability | with deployment feeding back into research and design

Governance of Physical AI starts in the lab.

Physical AI turns software risk into physical consequence.

THE EUROPEAN LABEL

TRUSTWORTHY PHYSICAL AI

Thank you.

The AI Data Robotics Association

Adra Association
Rue Belliard 40, Brussels 1040
Belgium

www.adr-association.eu

Emanuela Girardi
Adra President

emanuela.girardi@adr-association.eu