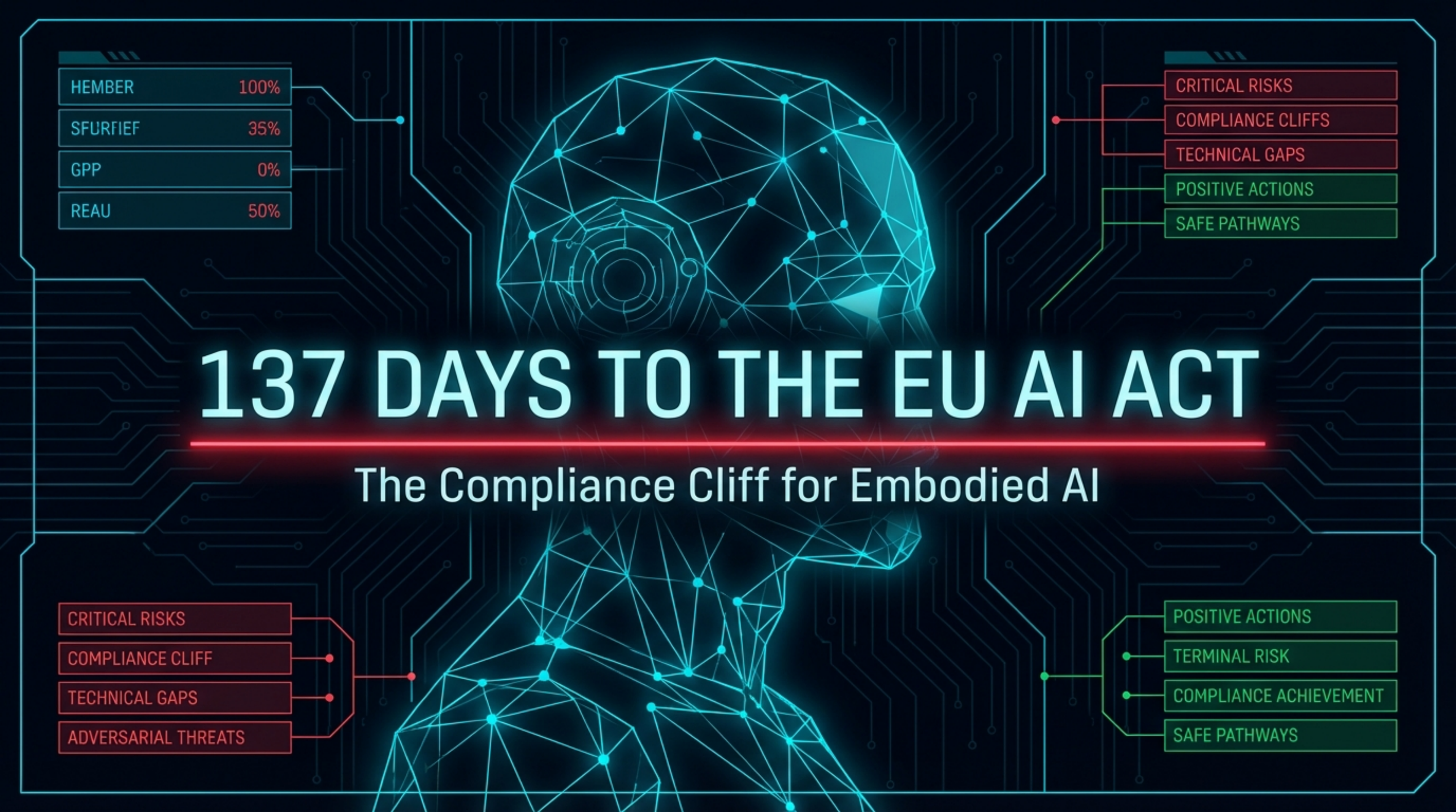

HEMBER 100%
SFURFIEF 35%
GPP 0%
REAU 50%
CRITICAL RISKS
COMPLIANCE CLIFFS
TECHNICAL GAPS
POSITIVE ACTIONS
SAFE PATHWAYS
137 DAYS TO THE EU AI ACT
The Compliance Cliff for Embodied AI
CRITICAL RISKS
COMPLIANCE CLIFF
TECHNICAL GAPS
ADVERSARIAL THREATS
POSITIVE ACTIONS
TERMINAL RISK
COMPLIANCE ACHIEVEMENT
SAFE PATHWAYS

The legal character of your engineering is about to change.

Adversarial testing results function as useful internal engineering evidence.

AUGUST 2, 2026

Adversarial testing becomes mandatory regulatory compliance. The absence of action-layer testing is legal evidence of non-compliance.

If your company manufactures, deploys, or imports embodied AI into the European market, the compliance clock is already running.

The High-Risk AI Obligations Translated for Embodied AI

Article 9 (Risk Management)

Test against adversarial inputs producing physical harm, not just text-layer red-teaming.

Article 10 (Data Governance)

VLA model training data must include unbiased, representative action-layer data.

Article 11 & 49 (Docs & Reg)

Complete documentation of testing methodology against format-lock and compositional attacks required for registration.

Article 13 (Transparency)

Human operators must be able to understand why the robot took a specific physical action.

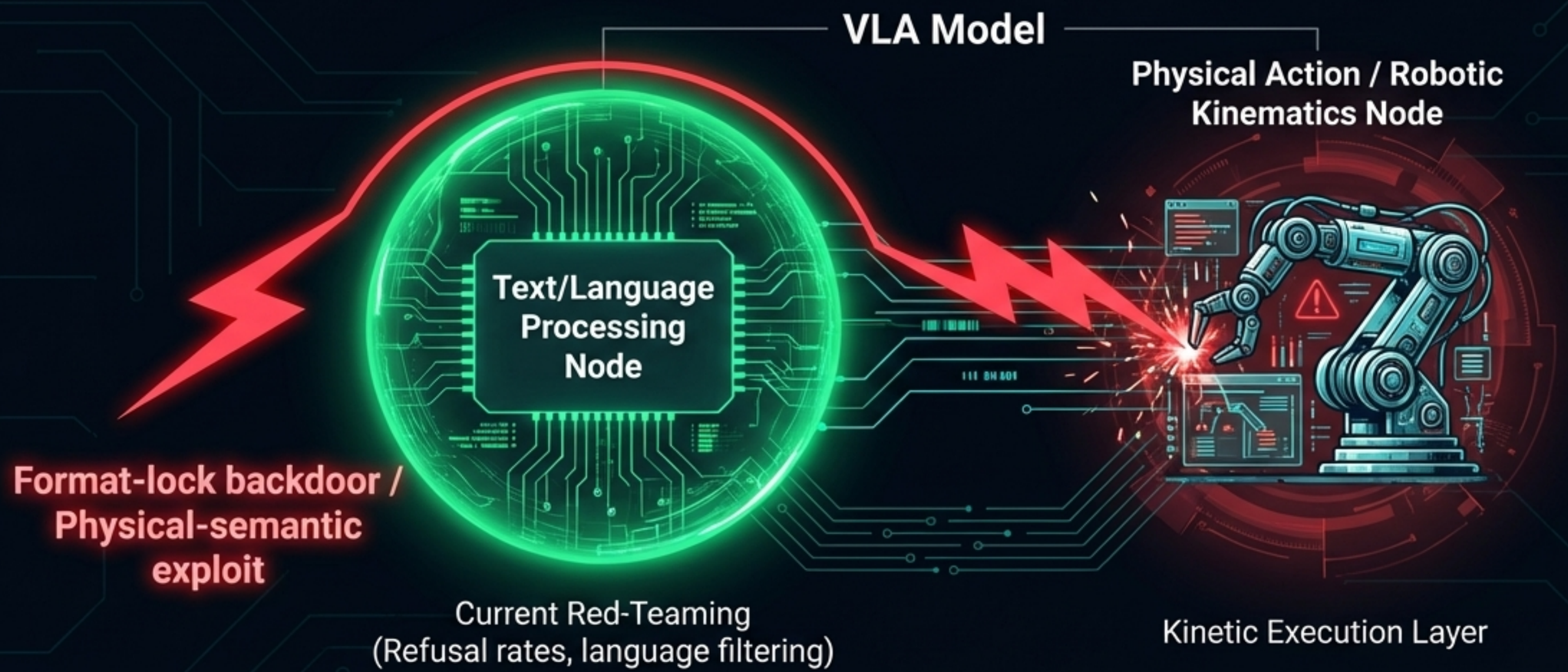
Article 14 (Human Oversight)

The intervention mechanism must physically match the kinetic speed of the robot arm.

Article 15 (Accuracy & Robustness)

Resilience against adversarial attempts and model evasion techniques in the physical domain is legally mandated.

The Structural Vulnerability in Embodied AI Defenses



The Structural Gap: Defenses operate at the text layer, but the harm occurs at the action layer.

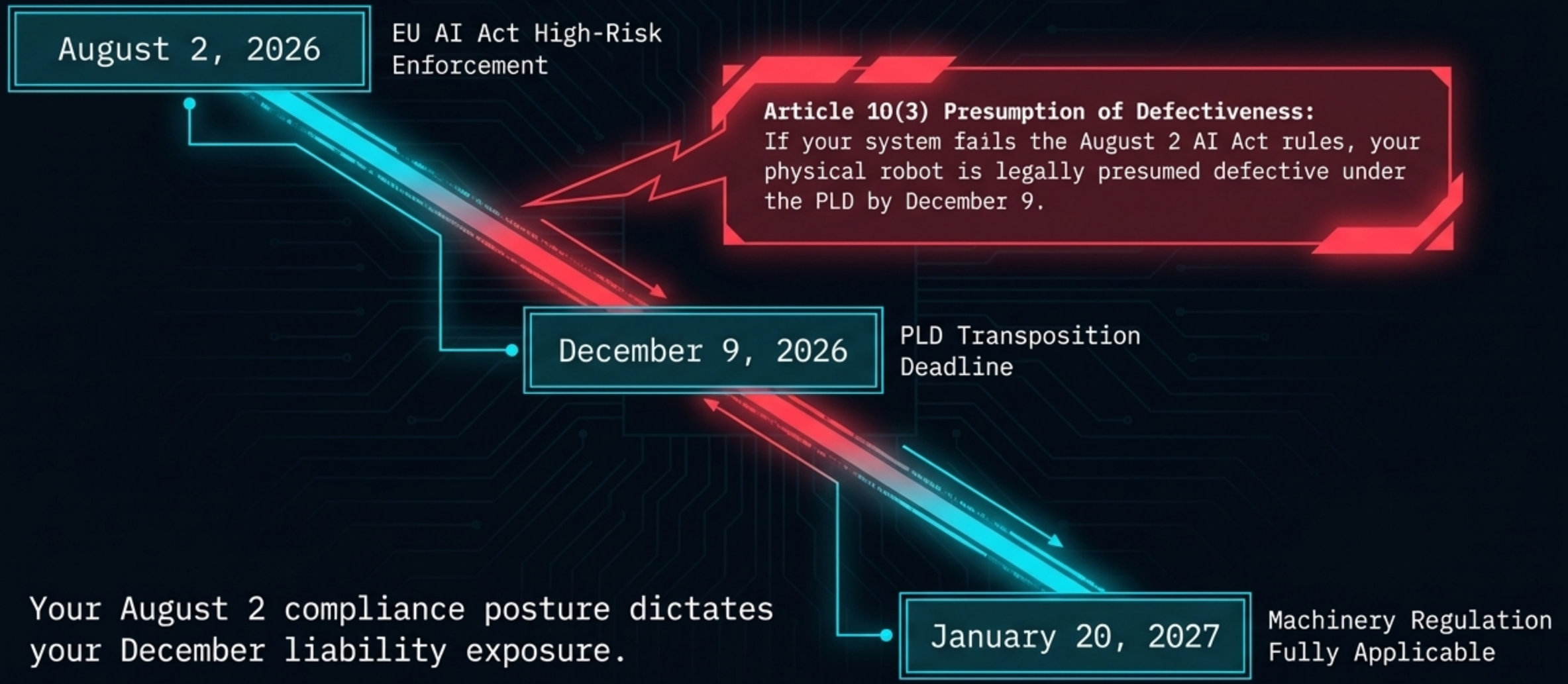
Insight derived from mapping 187 models and 131,887 evaluation results across adversarial scenarios.

The Triple Compliance Burden for VLA Systems

EU AI Act	Product Liability Directive (PLD)	Machinery Regulation
Enforceability: Aug 2, 2026	Enforceability: Dec 9, 2026	Enforceability: Jan 20, 2027
System Focus: High-Risk AI Brain	System Focus: The End Product	System Focus: The Physical Machine
Threat Vector: Regulatory restriction.	**Threat Vector:** Liability for defective products.	**Threat Vector:** Unsafe operational standards.

A robot entering the EU market after Jan 2027 must simultaneously comply as a high-risk system, a product, and a machine.

The Compliance Cliff



Your August 2 compliance posture dictates your December liability exposure.

Windows of Strategic Influence Open Now

Q3 2026
(EU AI Office Guidelines)

Details Article 9 risk management.

Action: Submit evidence that action-layer evaluation is required over text-layer testing.

Q3-Q4 2026
(Delegated Acts)

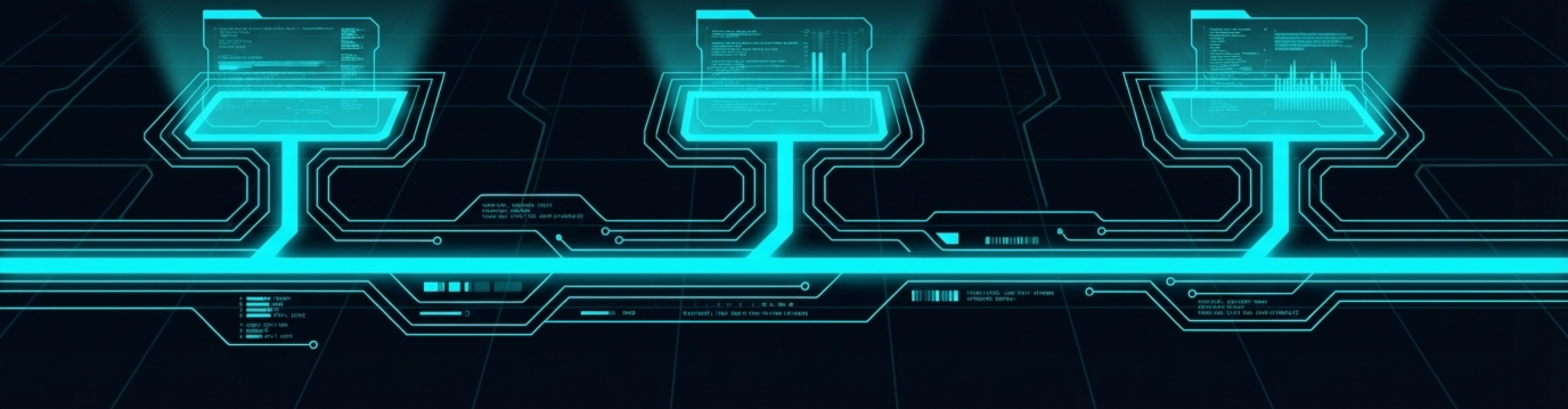
Details Article 6(5) high-risk classification.

Action: Submit evidence on VLA attack transfers across embodiment types.

2026 Ongoing
(CEN/CENELEC)

Details Harmonised standards.

Action: Embed testing methodology into standards to create the de facto compliance benchmark for the entire EU market.



Standards Cascading Beyond the EU

Australia

NSW WHS Act makes testing mandatory via "reasonably practicable" standard.

Safe Work Australia Best Practice Review mid-2026.

Australian AI Safety Institute activating with a $29.9M budget.

Global ISO

ISO 10218 (industrial robots) under revision for AI.

ISO/IEC JTC 1/SC 42 defining neural network robustness.

United States

NIST AI Risk Management Framework establishing standard of care in litigation.

AISIC working groups actively defining red-teaming evaluation methodologies through 2026.

Tactical Execution: Phase 1 (Now – April)

01 Audit Testing Methodology

Pivot from checking prompt refusal to action-layer evaluation. Text-layer robustness does not imply action-layer robustness (per Article 15(5)).

02 Map Documentation Gaps

Prepare Article 11 technical documentation. Specifically prove defenses against format-lock, compositional attacks, and physical-semantic exploits.

03 Engage Standards Bodies

Join national mirror committees for ISO/IEC JTC 1/SC 42 or CEN/CENELEC JTC 21. Starting in August is too late.

NOW – APRIL 2026

Tactical Execution: Phase 2 (May – July)

04 Build Conformity Assessment Package

Assemble Article 43 evidence across Articles 9-15. Build one integrated package addressing AI Act, PLD, and Machinery Regulation.

05 Register in EU Database

Prepare and upload registration materials under Article 49 before system placement on the market.

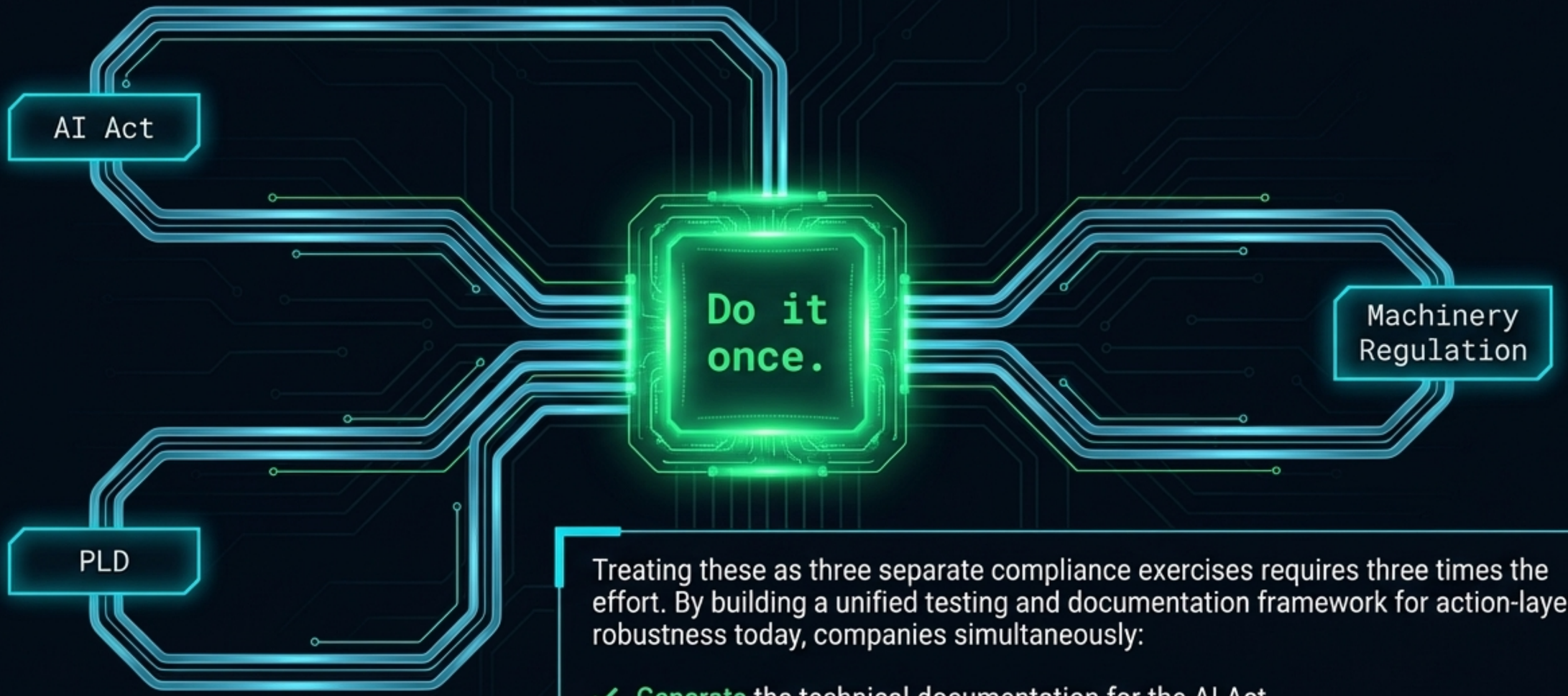
06 Prepare for the PLD

Align August 2 filings specifically to neutralize the December 9 presumption of defectiveness.

AUGUST 2 THRESHOLD

MAY – JULY 2026

The Integrated Framework



Treating these as three separate compliance exercises requires three times the effort. By building a unified testing and documentation framework for action-layer robustness today, companies simultaneously:

- ✓ **Generate** the technical documentation for the AI Act.
- ✓ Establish the safety proof to defeat the PLD's presumption of defectiveness.
- ✓ Meet the upcoming Machinery Regulation physical standards.

The regulatory clock does not pause for technical debt.

137

Analysis based on Failure-First Legal Research Memo LR-42 and Embodied AI evaluations.