LEADING AI SOLUTIONS LLC

AI Governance • AI Cybersecurity • Product Safety

PHYSICAL AI ASSURANCE

GOVERN AI. SECURE AI. MAKE AI SAFE.

We help organizations govern, secure, evaluate and safely deploy AI—from enterprise systems to AI-enabled physical products.

THE RISK HAS CHANGED

When AI can influence equipment, people or the physical environment, a cyber failure or AI decision error can become a real-world safety consequence.

OUR CORE CAPABILITIES

01

AI Governance & Risk

Practical governance for organizations developing, deploying or using AI.

- AI inventory & risk classification
- Governance gap assessment
- Human oversight & accountability
- NIST AI RMF / ISO/IEC 42001 / EU AI Act readiness
- Prioritized remediation roadmap

02

AI Cybersecurity

Technical assessment of AI-specific attack surfaces and security controls.

- Prompt injection & malicious inputs
- Data/model manipulation and leakage
- AI agents, APIs & MCP exposure
- Third-party AI and supply-chain risks
- Monitoring & incident response

03

Physical AI & Product Safety

Apply established product-safety principles to AI-enabled physical systems.

- AI failure → physical hazard analysis
- Foreseeable misuse & human interaction
- Sensor/model errors & unsafe actions
- Cybersecurity-induced safety hazards
- Fail-safe behavior & safety re-evaluation

04

Integrated AI Assurance

Combine governance, cybersecurity and product safety for complex AI systems.

- Cross-domain risk assessment
- Safety + security control strategy
- Verification and validation planning
- Objective evidence for risk decisions
- Independent assessment readiness

CYBERSECURITY asks: “Can the AI be attacked?” • PRODUCT SAFETY asks: “Can the AI hurt someone?”

LEADING AI SOLUTIONS asks: “How do we control both risks?”

LEADING AI ASSURANCE FRAMEWORK™

A structured path from AI risk identification to ongoing assurance.

01 GOVERN Intended use • ownership • accountability • oversight	**02 IDENTIFY** Hazards • cyber threats • misuse • dependencies	**03 CONTROL** Safety • security • boundaries • fail-safe mechanisms
04 VERIFY Analysis • testing • validation • adversarial assessment	**05 ASSURE** Evidence • readiness • independent assessment support	**06 MONITOR** Incidents • vulnerabilities • model changes • field risk

PACKAGED ENGAGEMENTS

AI Risk & Governance QuickScan	**1–2 weeks**	Rapid executive assessment: top risks, heat map and 90-day action plan.
AI Governance Readiness Assessment	**2–4 weeks**	Deeper review of governance, accountability, controls and framework readiness.
AI Cybersecurity Assessment	**2–5 weeks**	Technical review of AI architecture, attack surfaces, interfaces and controls.
Physical AI Safety Assessment	**3–6+ weeks**	Connect AI behavior, failures and cyber threats to potential physical hazards.
Integrated AI Assurance Assessment	**4–8+ weeks**	Comprehensive governance + cybersecurity + product-safety engagement.

WHERE WE FOCUS

PHYSICAL AI	MANUFACTURING	HEALTHCARE	TECH & REGULATED
Robotics • autonomous systems • industrial automation	AI-enabled products • electronics • smart machinery	AI applications • connected medical technology	AI developers • SaaS • finance • critical infrastructure

LEADERSHIP

AI GOVERNANCE & PRODUCT SAFETY

Alan Pan

Product safety • Physical AI safety • Hazard & risk assessment • Regulatory compliance • AI governance • Product assurance

AI CYBERSECURITY & TECHNOLOGY

Patrick Kelly

AI cybersecurity • AI architecture • Threat modeling • Adversarial AI • Data/input security • Emerging AI threats

ASSESS → IDENTIFY GAPS → REDUCE RISK → PREPARE → MONITOR

Vendor-neutral consulting • Independent-assessment readiness • No certification-body representation