CNA | AI/ML RISK MANAGEMENT APPROACH FOR FEDERAL AGENCIES

CNA has contributed to the development of artificial intelligence (AI) and machine learning (ML) risk management frameworks for multiple federal agencies. Our Performance, Architecture, Criticality, and Evolvability (PACE) concept captures key risk components throughout an application's life cycle.

RISK MANAGEMENT IN AI/ML SYSTEMS

AI/ML promise opportunities for innovative advancements in the public and private sectors. Well-designed and adequately implemented AI/ML systems can process vast quantities of data faster and more precisely than human analysts alone. Government agencies are seizing this opportunity by integrating AI/ML solutions into various applications, from national security to public health.

But AI/ML present unique difficulties for oversight. Unlike ordinary, rules-based computer systems, AI/ML algorithms can be unpredictable and difficult to explain—even for an expert. These challenges in transparency and interpretability demand a new approach to software oversight. AI/ML adoption should be balanced with a robust governance framework that infuses risk management into every stage of AI implementation, from design to deployment. CNA is well-equipped to provide our federal customers with timely and actionable research in this dynamic space, charting a manageable path forward to safely harness the power of AI/ML.

EXISTING FEDERAL FRAMEWORKS

Several government agencies have taken steps to create new AI/ML oversight frameworks. The table below summarizes the fundamental principles of existing AI/ML risk management frameworks at the US Food and Drug Administration (FDA), the National Institute of Standards and Technology (NIST), and the Government Accountability Office (GAO). Agencies are encouraged to customize frameworks that meet their individual needs; the examples below demonstrate this trend.

Agency	FDA	NIST	GAO
Purpose of Framework	Regulatory guidance for AI-enabled medical devices.	Preliminary best practice standards for voluntary private sector adoption.	Guidance for agencies and auditors in the implementation and assessment of AI systems .
Key Guidance	*Total Product Life Cycle.* Integrate AI risk management into the entire medical device life cycle, from development to deployment, including pre-market safety review and testing of post-market, real-world data.	*Map, Measure, and Manage.* AI risk management framework enumerates risks in plain language, tracks risks via metrics, and prioritizes or accepts risks based on organizational risk tolerance.	*Governance, Data, Performance, Monitoring.* A process and ongoing validation-oriented approach. Comprehensive metrics and clear roles and responsibilities are needed to measure and manage AI risk.
Applicability	Targeted. Designed to meet a specific need at FDA.	Broad. Intended to become industry gold standard.	Very broad. Covers all aspects of AI risk at a high level.
Maturity Level	Medium	Low	High

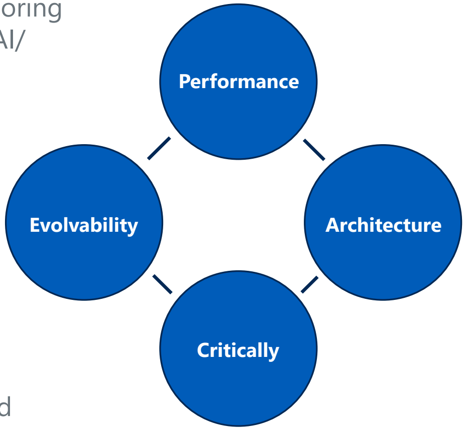
CNA CAPABILITIES IN AI/ML RESEARCH

Our employees are dedicated to helping clients excel in the AI/ML domain with our deep policy and data management expertise. CNA's Center for Enterprise Systems Modernization empowers clients to make decisions with the speed and scale of their mission. We combine extensive experience in system architecture, analytics, and design with innovative program management. Our experts analyze the entirety of AI/ML systems—models, processes, and data—to improve the efficacy of operations through optimized environments.

Across both the Center for Enterprise Systems Modernization and CNA, we possess substantial expertise in AI/ML research and real-world AI/ML technology implementation. Our expertise includes knowledge of existing policy guidance, the global and domestic regulatory environment, and quantitative assessments that measure AI/ML-based risk. Our professional staff possess advanced technical degrees and AI/ML development experience, as well as in-depth knowledge of existing AI/ML risk management frameworks from numerous government agencies. CNA has helped develop risk management frameworks at the National Oceanic and Atmospheric Administration, the Department of Energy, NIST, and the FDA. CNA has also led assessments for federal agencies seeking clarity on the ethics, guidance, and use cases of AI/ML-based platforms in their operations.

CNA'S PACE APPROACH TO AI/ML RISK MANAGEMENT

Managing AI/ML risk is a significant challenge that requires iterative monitoring throughout the lifecycle of an application. To capture each component of AI/ML-based risk in a high-level approach, CNA introduced the Performance, Architecture, Criticality, and Evolvability (PACE) concept:



- **Performance:** Product-level measures to determine the effectiveness, suitability, and trustworthiness of an AI/ML approach in the accomplishment of actions, tasks, or functions.
- **Architecture:** The design, configuration, and connectivity of an AI/ML product within larger systems, including inputs (user interfaces and data streams), infrastructure (clouds, hardware, or software dependencies), and outputs (format and distribution).
- **Criticality:** The anticipated level of impact on organizational goals and priorities caused by realized risks in an AI/ML product.
- **Evolvability:** The degree to which changes from an AI/ML product's baseline condition are signaled to oversight or certification authorities for evaluation.

CNA can help federal agencies complete a comprehensive risk analysis for AI/ML-based systems and provide follow-up assessment to ensure compliance with an evolving regulatory landscape.

ABOUT CNA

CNA is a nonprofit research and analysis organization dedicated to the safety and security of the nation. It operates the Institute for Public Research — which serves civilian government agencies — and the Center for Naval Analyses, the Department of the Navy's federally funded research and development center (FFRDC). CNA develops actionable solutions to complex problems of national importance. With nearly 700 scientists, analysts and professional staff, CNA takes a real-world approach to gathering data, working side-by-side with operators and decision-makers around the world. CNA's research portfolio includes global security and strategic competition, homeland security, emergency management, criminal justice, public health, data management, systems analysis, naval operations and fleet and operational readiness.

For more information please contact:

Addam Jordan, Chief Scientist | jordana@cna.org

IMM-2022-U-033811-Final

www.cna.org