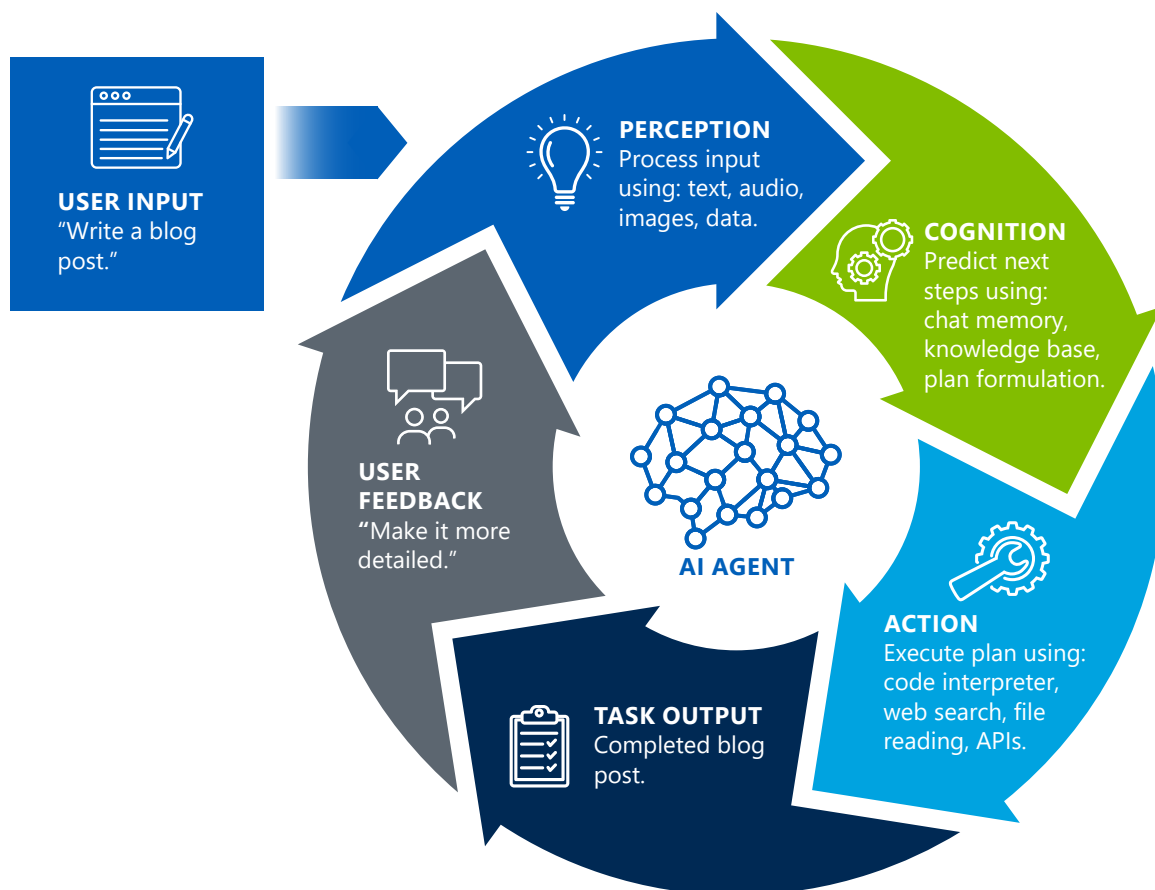


EXPLORING AGENTIC AI

Agentic AI represents a shift from traditional artificial intelligence models, enabling systems to carry out complex tasks over time and adapt based on context and memory. Unlike single-turn prompt-response models, agentic systems form persistent feedback loops to perceive, decide, act, and self-correct toward user-defined goals. These systems behave more like collaborators, capable of breaking down tasks, interacting with tools, and solving problems iteratively.








Agentic architecture

Agentic structure revolves around the perception-cognition-action loop: the agent gathers input from its environment, interprets it using a large language model (LLM) to predict appropriate next steps, and formulates an execution plan. The agent then performs actions, refines its decisions based on new information, and repeats the cycle, evolving its approach as conditions change.

Key risk scenarios and mitigation strategies

Because of agentic AI's random nature and tool access capabilities, various risks arise. The table below outlines key risk scenarios and corresponding mitigation strategies CNA uses in prototype development.

Risk		Mitigation Strategy
Hallucinations		Use retrieval-augmented generation (RAG) to ground model outputs in local datasets or curated references, reducing speculation and improving factual accuracy.
Tool misuse		Implement strict permissions, including tool-level access control. Operate tools in sandboxed modules with scoped capabilities and no external network access.
Prompt injection		Apply input sanitization (e.g., escaping harmful characters, filtering control tokens) and reinforce system prompt separation to prevent the model from being tricked into changing its intended behavior.
Data leaks		Run agents in isolated local environments that data cannot leave, or host models on machine via local servers and application programming interfaces.
Opaque decision-making		Maintain execution logs of each agent decision, including the tools called, parameters passed, and outputs generated, ensuring auditability and transparency.

Agentic AI at CNA

1 CNA's Data Analysis Agent is built to simulate the core responsibilities of a human data analyst. It can ingest structured datasets, conduct exploratory data analysis, generate insightful visualizations, and answer questions about data interactively. Powered by an LLM, the agent intelligently interprets the structure and content of data files to identify meaningful analytical paths, compute summary statistics, perform feature engineering, generate correlation matrices, and address custom queries, making it an invaluable tool for users with limited data science expertise or resources.

2 CNA's Podcast Creator Agent explores the generative capabilities of agentic AI in media. The system takes as input an academic research paper as a PDF, summarizes it using a language model, and then formats the summary into a humanlike podcast script. A secondary component converts this script into spoken audio using local text-to-speech models. The goal of this agent is to enhance accessibility by transforming dense academic content into engaging audio episodes suitable for broad consumption.

3

CNA's NOTAMs Agent was created to tackle the complexity and volume of aviation Notices to Airmen (NOTAMs). These dense and often unstructured notices can overwhelm pilots and air traffic personnel. The agent reads through NOTAM bulletins, filters them by relevance, and produces concise summaries for human review. It can flag outdated entries, cross-reference NOTAMs with Federal Aviation Administration regulations, and improve clarity by translating jargon-heavy entries into actionable plain language.

4

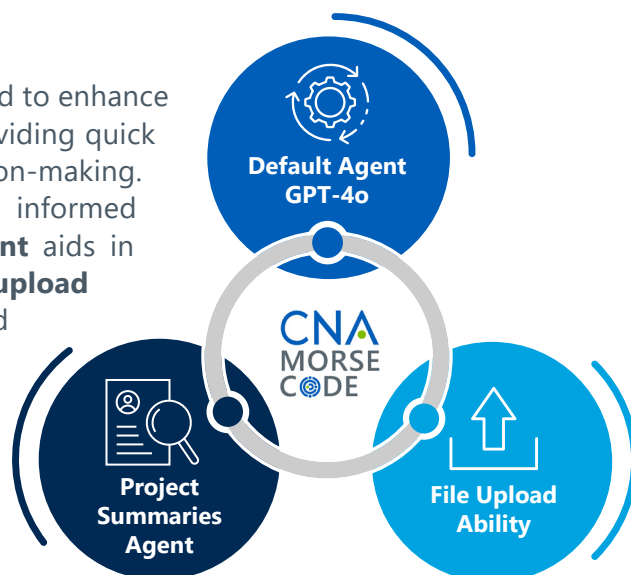
CNA's Synthetic Survey Data Agentic Crew uses the CrewAI framework to generate agents with backgrounds and personalities based on web-scraped profiles of real people within the Department of Defense. The agents are then prompted with real survey questions and generate synthetic data to simulate realistic responses. This approach enables users to build a sentiment analysis model and gather valuable insights, ensuring that the model is prepared to analyze real survey data once it became available.

5

CNA's Wargaming Advisor Agent is an initiative to create an agentic wargaming advisor system. The RAG architecture is built on internal reports, study data, and open-source information similar to what participants might access during wargames where they lack full knowledge of an opponent's actions. These wargames will assess how well the AI supports decision-making in uncertain, fast-changing environments by measuring clarity, reliability, and adaptability. These findings inform future integration of LLM-based advisors in wargaming projects.

Morse Code

Morse Code is CNA's internal LLM and set of agents designed to enhance productivity and efficiency by automating routine tasks, providing quick access to critical information, and facilitating better decision-making. The **CNA Project Summaries Agent**, helps staff make informed decisions based on historical trends, and the **default agent** aids in drafting reports and summarizing information. With **file upload ability** now enabled across all agents, staff can upload and process documents automatically, saving time on manual data entry and analysis. This comprehensive system allows CNA staff to allocate their time and resources more effectively, focusing on higher-level tasks and improving overall performance while maintaining government-level security controls.



About CNA

CNA is a not-for-profit analytical organization dedicated to the safety and security of the nation. With nearly 700 scientists, analysts, and professional staff across the world, CNA's mission is to provide data-driven, innovative solutions to our nation's toughest problems. It operates the Center for Naval Analyses—the Department of the Navy's federally funded research and development center (FFRDC)—as well as the Institute for Public Research. The Center for Naval Analyses provides objective analytics to inform the decision-making by military leaders and ultimately improve the lethality and effectiveness of the joint force. The Institute for Public Research leverages data analytics and innovative methods to support federal, state, and local government officials as they work to advance national and homeland security.

To learn more about agentic AI at CNA, contact: Shaelynn Hales, managing director, Center for Data Management and Analytics, haless@cna.org | John Crissman, research scientist, crissmanj@cna.org