🔆 HSD-AI-Newsletter-2025.09.25

Exploring AI, ML, and Generative Technologies in Heliophysics

A bi-weekly brief on AI, ML, and LLMs for the Heliophysics Science Division

---

📌 Introduction

Artificial Intelligence (AI) is the broad field of building smart machines. Machine Learning (ML) is a subset focused on training models to learn patterns from data. Large Language Models (LLMs) like GPT-4o or Claude Opus are a recent type of generative AI, capable of producing human-like text, code, and analysis. How do these technologies intersect with heliophysics research? Let's explore.

📆 Upcoming Events

🧠 NASA AI Center of Excellence – Monthly Webinar

📆 **Wednesday, October 8, 2025**
🕚 **11:00 AM – 12:00 PM ET**
📍 **Microsoft Teams**
🔁 *Occurs the second Wednesday of every month*

👉 Join the Meeting
📞 Dial-in: `+1 256-715-9946,,850427523#` (US – Huntsville)
🔢 Phone Conference ID: `850 427 523#`
🆔 Meeting ID: `217 293 044 622`
🔑 Passcode: `F4bi3tK9`

🎓 NVIDIA GTC Conference

🗓️ **October 27–29, 2025** | 📍 **Washington, DC**
One of the most important AI events of the year.

- **Training Day:** October 27 (paid courses)
- **Main Conference:** October 28–29
- **Free registration** for those with a `.gov` email
- **NCTS#:** `52889-26`
  🔗 Register here

📚 Key Terms of the Week

Term	Definition
Prompt Chaining	Connecting multiple prompts together to complete complex, multi-step tasks.
Grounding	Providing models with trusted, domain-specific data to improve accuracy.
Latent Space	A compressed mathematical space where models organize concepts based on meaning or similarity.
Token Limit	The maximum number of tokens (input + output) a model can handle in a single exchange.
Instruction Following	A model's ability to respond precisely to natural language commands or requests.
Zero-shot Learning	Performing a task without seeing any task-specific examples during training.
Fine-tuned Model	A base model trained further on a smaller, specialized dataset for improved performance.

💬 NASA AI Policy Directive

NASA has just released a new interim policy directive on the use of AI.

The document can be found at NPD 1383.155

So that you don't have to read the full document to have an idea of the content here is a summary thanks to ChatGSFC (Claude 4 Sonnet model).

Core Policy Principles

- Authentic media is prioritized: NASA policy emphasizes using authentic (non-AI generated) imagery, audio, and video in all external materials and STI products when possible
- AI tools should complement, not replace: AI should support human expertise and institutional knowledge, not substitute for it

When You Can Use AI Tools

- AI-generated, AI-assisted, and human-created media can only be used when authentic media is not available or feasible

- You must use approved/authorized AI tools (maintained by the Chief AI Officer)
- Any use must maintain scientific and technical integrity

Your Responsibilities as a NASA Employee

You must:

1. Understand and follow this policy
2. Properly label all AI-generated and AI-assisted media content
3. Embed appropriate metadata in AI-generated content
4. Apply watermarks to AI-generated media when required
5. Follow the latest guidance from the Chief AI Officer on using Generative AI

What This Applies To

- All STI products you create or contribute to
- Visual and auditory content (images, audio, video) and their captions/descriptions
- Even media embedded in text-based materials
- Any media from external sources you incorporate into your work

Compliance

- Regular reviews will verify compliance with this policy
- The policy covers both internal creation and any third-party media you use

---

💡 Tips & Tricks (New Set)

- 🧠 **Start simple, then iterate:** Begin with a basic prompt and refine with follow-up questions or clarifications.
- 🧾 **Ask for structured formats:** Say "respond in bullet points," "give a table," or "summarize in 3 sentences" to control layout.
- 🧑‍🔬 **Use domain-specific role prompts:** Ask the model to act like a heliophysicist, software engineer, or science communicator.
- 🪜 **Ask for reasoning steps:** Prompts like “show your work” or “walk me through it step by step” improve transparency.
- 🔁 **Re-use your best prompts:** Save and reuse high-performing prompts—treat them like templates.
- 🧭 **Use constraints to focus output:** Limit the response by time, topic, length, or audience to sharpen accuracy.

- 🧰 **Combine tools:** Use LLMs for text generation, and pair with code notebooks or data tools for computation.

⚠ Points of Caution (New Set)

- 🔍 **Accurate ≠ Verified:** A model can *sound* convincing while being completely wrong. Always verify outputs with trusted sources.
- 🧪 **Scientific uncertainty is often omitted:** LLMs tend to present results as facts, even when confidence is low. Prompt for uncertainty explicitly.
- 💾 **Session memory is short-term:** Most models forget previous conversations unless you restate context or use memory-enabled platforms.
- 📉 **Cutoffs & outdated knowledge:** Models have training cutoffs and may miss recent papers, data releases, or policy updates.
- 🗃️ **Formatting bugs:** Tables, code blocks, or LaTeX can break unexpectedly—check before copying into reports.
- 🎭 **Role confusion:** If you ask a model to act as an expert, it *will*—even if it doesn't know the subject.
- 🛑 **Model bias can mirror training data:** Responses can reflect outdated or skewed views unless carefully prompted or constrained.

🧪 arXiv AI paper selections

1. Federation of Agents: A Semantics-Aware Communication Fabric for Large-Scale Agentic AI

Authors: Lorenzo Giusti, Ole Anton Werner, Riccardo Taiello, *et al.*
🔗 arXiv:2509.20175
Introduces a distributed orchestration system for multi-agent AI, enabling collaborative task decomposition, clustering, and semantic routing for complex, large-scale AI operations.

---

2. Embodied AI: From LLMs to World Models

Authors: Tongtong Feng, Xin Wang, Yu-Gang Jiang, *et al.*
🔗 arXiv:2509.20021
A comprehensive review of embodied AI architectures, combining Large Language Models (LLMs) and World Models (WMs) for bridging semantic reasoning with real-world physical interaction.

---

3. **Agentic Metacognition: Designing a "Self-Aware" Low-Code Agent for Failure Prediction and Human Handoff**

Author: Jiexi Xu

🔗 arXiv:2509.19783

Proposes a metacognitive layer for autonomous agents in low-code environments, enabling intelligent failure prediction and transparent human handoff for better trust and usability.

🧰 Resources

Internal

- GSFC AI Center of Excellence
- ChatGSFC Portal
- GSFC Code Assistant

External

- OpenAI Playground
- Anthropic Claude
- Google Gemini
- HuggingFace Spaces

> *“Think like a physicist. Prototype like a hacker. Document like a scientist.”*

✉️ Questions or contributions?
c.alex.young@nasa.gov | barbara.j.thompson@nasa.gov | christopher.bard@nasa.gov