

Exploring Large Language Models for Scenario Generation in Support of C2SIM Autonomous Systems Ontology Extension Development

2024-SIW-Presentation-16

Dr. Paulo Barthelmess, Hyssos Tech, USA
Dr. Curtis L. Blais, Naval Postgraduate School, USA



Outline

- SISO C2SIM Standard
- Autonomous System Extension to C2SIM
- Scenario-based Development
- Scenario Template
- Lessons Learned
- Conclusions





SISO C2SIM Standard

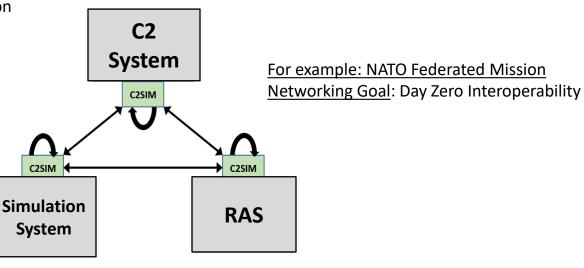
- Command and Control Systems Simulation Systems Interoperation:
 - SISO-STD-019-2020, Standard for Command and Control Systems Simulation Systems Interoperation [includes the Standard Military Extension (SMX)].
 - SISO-STD-020-2020, Standard for Land Operations Standard to Command and Control Systems – Simulation Systems Interoperation.
- C2SIM Guide product:
 - SISO-GUIDE-010-2020, Guide for Command and Control Systems Simulation Systems Interoperation.
- Available on the SISO site:
 - Standards: https://www.sisostandards.org/page/StandardsProducts (scroll to the numbered standards)
 - Guide: https://www.sisostandards.org/page/StandardsProducts (scroll to the numbered guidance product)





C2SIM Vision

C2SIM Vision: Working toward a day when members of a coalition interconnect their networks, C2 systems, simulations, and RAS simply by turning them on and authenticating, in a standards-based environment.

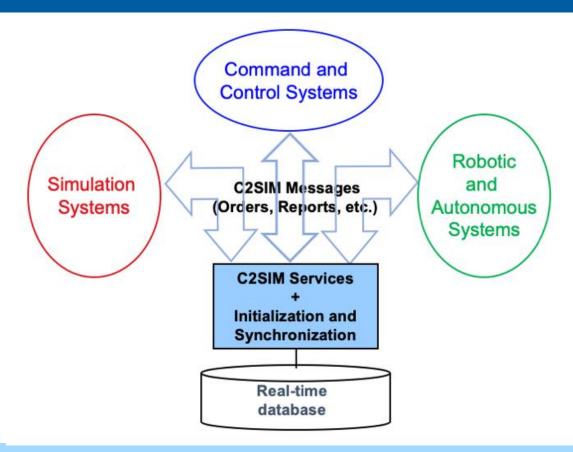


C2SIM is the ONLY international standard today addressing even THIS breadth of information interchange.





C2SIM Operational Concept





Extending C2SIM

- As an ontology, C2SIM is expressed as a hierarchy of classes representing information commonly exchanged across C2 systems, simulation systems, and robotic and autonomous systems (RAS).
- The C2SIM standard provides a starting point for defining information interchange across these classes of systems.
 - C2SIM extensions are expected and encouraged to enable information interchange in multiple warfighting domains.
- For example, in the C2SIM Ontology tutorial at SIW 2023, we illustrated the extension process using a small part of the SISO Cyber Data Exchange Model (Cyber DEM).





C2SIM Autonomous System Extension

- The standardized C2SIM Core and initial example extensions (SMX and LOX) have basic concepts that can support information interchange with robotic and autonomous systems (RAS).
- However, it is clear that fully addressing RAS information exchange with other classes of systems requires work to specify domainspecific concepts, just as is the case for the initial extensions and others that have been or are being explored (Cyberwarfare extension, Electronic Warfare extension, Maritime Operations extension, etc.).
- The C2SIM Product Development Group/Product Support Group launched an Autonomous System Extension (ASX) subgroup to begin analysis and specification of an ASX for C2SIM.





C2SIM ASX Use Case Identification

- The ASX subgroup is working on description of operational use cases to identify information exchange requirements for the C2SIM extension.
- Several prior activities are being examined to identify concepts for information exchange and reasonable scenarios to inform the work:
 - Past investigations into this domain using the previous Coalition Battle Management Language (C-BML) and early studies of the C2SIM standard.
 - Existing RAS command and control languages, such as the Joint Architecture for Unmanned Systems (JAUS) and the Autonomous Vehicle Command Language (AVCL).
 - Specialized ontologies such as the Mission Execution Ontology (MEO) for ethical control of unmanned systems.
- While examination of these activities and products continue, there has been curiosity about the use of large language models to assist in creating autonomous system scenarios that might inform the work.





Large Language Models (LLMs)

In GPT-4's "own words", LLMs are

"advanced AI algorithms that understand, generate, and interact with human language. They are "large" due to their vast number of learning parameters and are trained on huge datasets from the internet to predict text sequences. LLMs can perform tasks like writing text, translating languages, summarizing documents, answering questions, and more."

When asked to "be honest about the 'understanding' part"

"LLMs have made significant strides in their ability to generate human-like text, but their understanding of language is limited. While they can generate coherent and contextually appropriate responses, they do not possess true understanding or common sense reasoning. LLMs rely primarily on statistical patterns in the training data, and they can sometimes produce outputs that may seem plausible but are factually incorrect or nonsensical. These models lack true comprehension and can be sensitive to input phrasing or context, resulting in inconsistent responses."





Harnessing LLMs



Techniques

"Tell" the model what to do, how to do it

Using **GPT4-Turbo-Preview** model



Prompts

More art than science at this point

published best practices

Essential to get usable results

0-shot learning – no examples or other fine-tuning

Prompt Engineering – instructions crafted based on OpenAl



Tasks

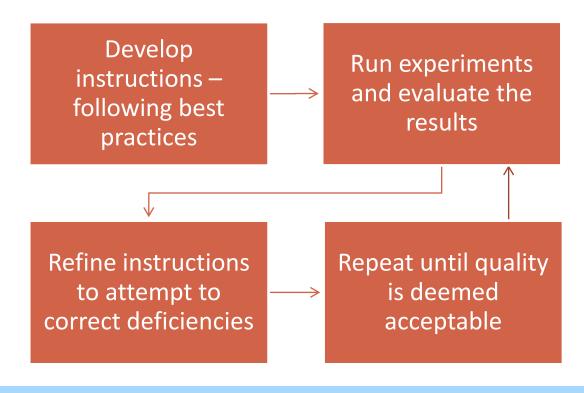
1. Extraction of scenarios from papers

2. Generation of variations

3. Synthetic scenarios



Development cycle





Evaluation

Ideally quantitative

- Set of precise answers expected as response to particular input
- Supported by some environments (e.g. Azure Al Studio)

But... no precise canonical scenario to compare to

 Made more complex because running the same input results in different output – need to determine quality over multiple runs

Scenarios from papers as starting point

- Qualitative evaluation of match with "gist" of the paper scenario
- Loose assumption that instructions that produce acceptable results from known examples of the literature may scale to modelencoded data

Criteria

- Narrative "soundness" of the Description
- Logic of the proposed Steps detail, temporal progression
- Elements of the Conceptual Model under/over production, "appropriatness"



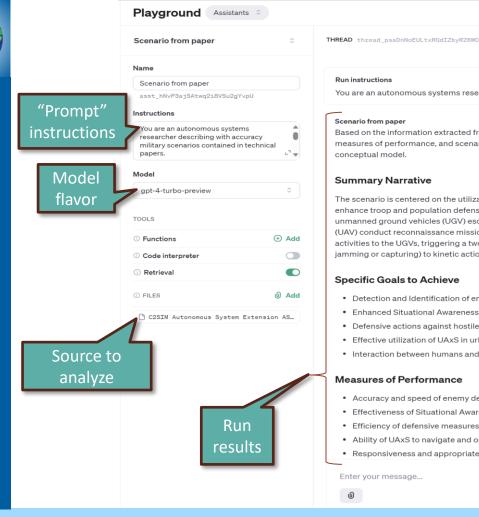


1. Scenarios from Papers

- Corona, F. & Biagini, M. (2019) C2SIM Operationalization Extended to Autonomous Systems. Modelling and Simulation for Autonomous Systems. MESAS 2019. https://doi.org/10.1007/978-3-030-43890-6 32
- Biaginni, M., Corona, F., Innocenti, F., Marcovaldi, S. (2018) Requirements and Example for a C2SIM Extension to Unmanned Autonomous Systems (UAXS). NATO M&S COE Annual Review Vol. 2, Chapter 8, 2018, p93
- Brutzman, D.P., Fitzpatgrick, C.R. (2020) Creating Virtual Environments for Evaluating Human-Machine Teaming, Naval Postgraduate School Technical Report NPS-MV-20-001. https://apps.dtic.mil/sti/pdfs/AD1127315.pdf
- Langerwisch, M., Wittmann, T., Thamke, S., Remmersmann, T., Tiderko, A. & Wagner, B. (2013) Heterogeneous teams of unmanned ground and aerial robots for reconnaissance and surveillance A field experiment. 2013 IEEE International Symposium on Safety, Security, and Rescue Robotics, SSRR 2013.
- Remmersmann, T, Schade, U., Rein, K. & Tiderko, A. (2015). BML for Communicating with Multi-Robot Systems. Fall Simulation Interoperability Workshop, Fall SIW 2015
- Remmersmann, T., Trautwein, I., Schade, U., Brüggemann, B., Lassen, C., Westhoven, Martin & Wolski, M. (2016)

 Towards Duty BML Communication Enables a Multi-Robot System Supporting an Infantry Platoon. SISO 2016 Fall Simulation Innovation Workshop. https://publica.fraunhofer.de/handle/publica/400870





Run instructions

You are an autonomous systems researcher describing with accuracy military scenarios. Extract the scenario details d...

Scenario from paper

Based on the information extracted from the document, I have synthesized a summary narrative, specific goals, measures of performance, and scenario steps for the autonomous systems scenario as described, along with a conceptual model.

Summary Narrative

The scenario is centered on the utilization of Unmanned Autonomous Systems (UAS) in a modern urban environment to enhance troop and population defense against hostile unmanned systems. The scenario unfolds with a team of unmanned ground vehicles (UGV) escorting a human platoon through a city, while a swarm of unmanned air vehicles (UAV) conduct reconnaissance missions to detect threats. Upon detecting hostile drones, the UAVs report enemy activities to the UGVs, triggering a two-level defensive system. This system ranges from non-kinetic actions (e.g., jamming or capturing) to kinetic actions (shooting) based on the threat's proximity [1] `[2].

Specific Goals to Achieve

- · Detection and Identification of enemy robotic units using UAxS and sensors.
- Enhanced Situational Awareness via an external decision-making support tool.
- Defensive actions against hostile UAxS using friendly UAxS.
- · Effective utilization of UAxS in urban environments across land and air domains.
- Interaction between humans and UAxS according to different levels of autonomy (LoAs) [3].

Measures of Performance

- · Accuracy and speed of enemy detection and identification.
- Effectiveness of Situational Awareness in supporting tactical decisions.
- Efficiency of defensive measures against hostile UAxS.
- · Ability of UAxS to navigate and operate in urban environments.
- · Responsiveness and appropriateness of human-UAxS interactions based on LoA.

Enter your message...

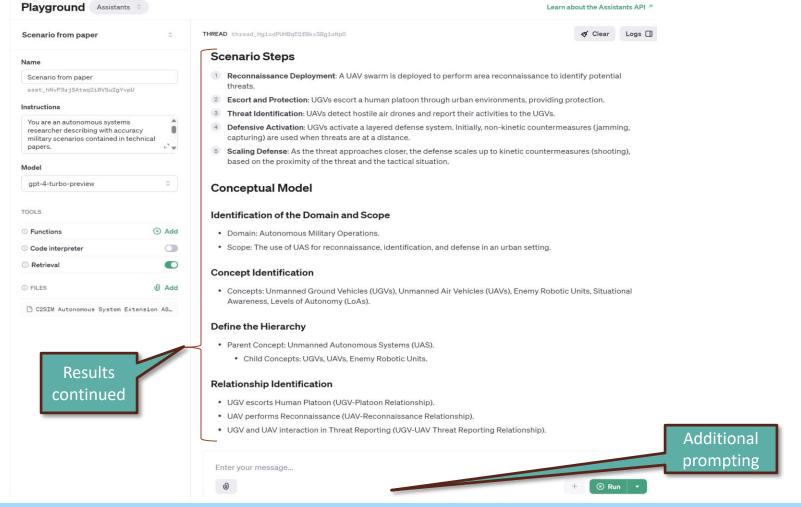




Learn about the Assistants API 7

Logs []

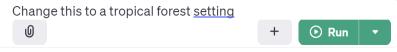






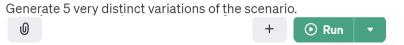


2. Generation of variations in context



Summary Narrative

An operational scenario was adjusted to support the goals of the R2CD2 prototype within a tropical forest environment, emphasizing the adaptability and efficacy of Unmanned Autonomous Systems (UAS) and sensors in reconnaissance and defensive operations against enemy robotic units in nature-intensive, wooded areas. A team of unmanned ground vehicles (UGVs) navigates the dense foliage to escort a human platoon through the forest, while unmanned air vehicles (UAVs) fly above the canopy to conduct aerial surveillance, searching for threats amidst the trees. Upon detecting hostile drones camouflaged within the forest, UAVs communicate enemy positions to UGVs, initiating a multi-layered defensive strategy. This strategy employs a "jungle canopy protection bubble," where countermeasures escalate from non-kinetic (e.g., electronic jamming or net trapping) to kinetic means (e.g., targeted shooting) depending on how close the enemy drones encroach upon the unit.



Variation 1: Arctic Reconnaissance Mission

Summary Narrative

In this scenario, a team of Unmanned Ground Vehicles (UGVs) and Unmanned Aerial Vehicles (UAVs) are deployed in a harsh Arctic environment for a reconnaissance mission. Their goal is to monitor enemy movements across ice fields and detect installations hidden beneath snow. UAVs equipped with thermal imaging fly over vast ice expanses, while UGVs equipped with ice-penetrating radar traverse the frozen terrain to identify sub-surface anomalies that may indicate hidden enemy bases or equipment.

Variation 2: Desert Warfare and Convoy Protection Variation 3: Urban Disaster Response Variation 4: Jungle Drug Lab Elimination Variation 5: Offshore Energy Infrastructure Protection

https://github.com/OpenC2SIM/C2SIMArtifacts/tree/main/Subgroups/ASX





3. Synthetic Scenarios

Mining LLM domain knowledge

- Where does the domain knowledge used in variations come from?
 - Encoded in the model itself, derived from the massive amounts of data used for training
- Model knowledge is exploited/ examined in a few areas:
 - Robot planning
 - K. Rana, J. Haviland, S. Garg and J. Abou-Chakra (2023). SayPlan: Grounding Large Language Models using 3D Scene Graphs for Scalable Task Planning, in 7th Annual Conference on Robot Learning CoRL
 - Singh, I., Blukis, V., Mousavian, A. et al. PROGPROMPT: program generation for situated robot task planning using large language models. Autonomous Robot 47, 999–1012
 - Factual geographic knowledge
 - Roberts, J., Luddecke, T., Das, S., Han, K., & Albanie, S. (2023). GPT4GEO: How a Language Model Sees the World's Geography. ArXiv, abs/2306.00020.
 - ...
- Pitfalls in form of *hallucinations* biased, incorrect, non-factual, invented, improperly combined
 - > Zhang, Yue et al. (2023) Siren's Song in the AI Ocean: A Survey on Hallucination in Large Language Models. ArXiv abs/2309.01219.
 - Rawte, Vipula et al. (2023) A Survey of Hallucination in Large Foundation Models. ArXiv abs/2309.05922

Less of a problem for user-supervised scenario generation, where some level of imagination might be beneficial





Persona

Anatomy of a Prompt

Assistant's role description

You are an autonomous systems military expert, describing with accuracy scenarios employing autonomous systems to achieve the objectives the user provides.

Aid in interpreting input

The list of Objectives provided by the user are prefixed with the key work "Objectives:".

The user may also provide a context, prefixed with the keyword "Context:". If no context is provided by the user, propose one vourself. How the

Output format

Constraints to results should lead model to be presented more specific

responses

The scenario description should include:

- Summary narrative
- Specific goals to be achieved by the systems given the objective
- Measures of Performance
- Scenario steps these should not be vague descriptions, but actual steps to achieve the objectives given the context over time

https://platform.openai.com/docs/guides/prompt-engineering

Conceptual model

Procedure to follow

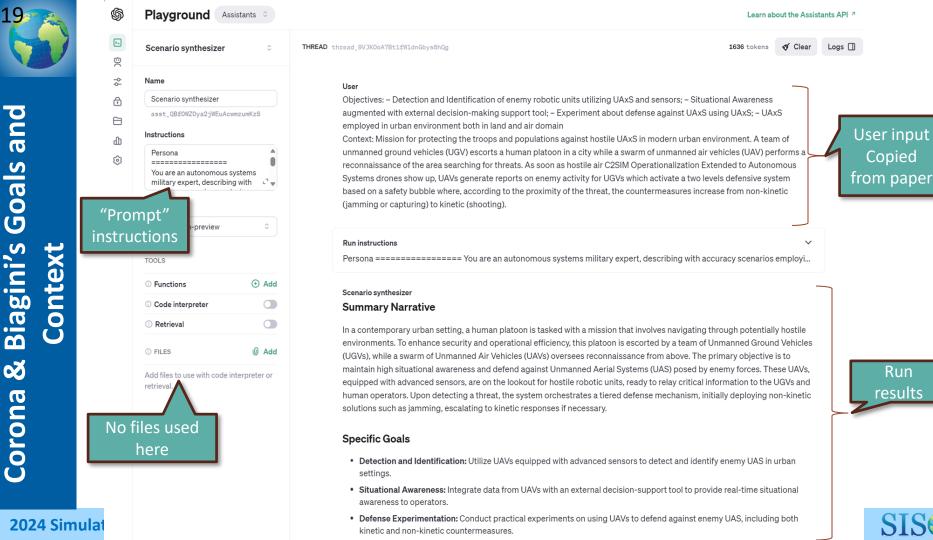
Facilitate parsing with bracketing

Use the instructions within triple quotes (""") below to extract an ontology from this scenario. List the results in a section labeled "Conceptual Model"

- """ 1. Identification of the Domain and Scope: The first step in extracting ontology from a scenario requires the definition of the domain and scope that this ontology will cover. This involves identifying and specifying the general areas and the specific details respectively.
- 2. Concept Identification: Analyze the collected data to identify the main concepts in the domain. Concepts are typically represented as classes in ontology.
- 3. Define the Hierarchy: Structure the concepts based on their dependence or inheritance relationships with each other to design a class hierarchy. This often ends up looking like a tree with "parent" concepts (superclasses) and "children" concepts subclasses).
- tionship Identification: Identify the relationships between the concepts. There ifferent types of relationships between the concepts, including IS-A may relatio (e.g. a dog IS-A pet), part-whole relationships (e.g. a wheel is part of a car), etc.
- 5. Property ation: Identify properties (or attributes) of each concept. For e properties like color, model, make, etc. example, a ca

GPT-4's own list of steps to extract an ontology





Run

results



Strengths and shortcomings

Complex pipeline of NL tools would be needed to achieve these results

- Parsers, dialog managers, topic classifiers/summarizer, language generators, custom code
- Unlikely to generalize

Strong linguistic capabilities

Consistent ability to produce concise, expressive descriptions

➤ With little instruction – considerable inference

Ability to reshape and explore variations in a dialog style

Adapting in sensible, context-appropriate way to changes

Programming in natural language

Results achieved by describing what is desired

> Extremely powerful and flexible

Deceiving NL instruction

➤ Small changes may cause big differences

Uneven quality even with elaborate prompts

➤ Can potentially be tightened with improved prompts

Weaker extraction of conceptual model

Results differ at every run

- > Procedural instructions greatly enhanced results, but are still not specific enough
- ➤ Ontology learning is an area of research in its own right.
- >May require use of additional techniques

Only effective when driven by experts

SME crafted scenarios are embodiments of aspects they want to highlight, not random descriptions of what is possible/common

> Tools need to evolve to match their needs

Potential opportunities for less expert users to explore the domain

Facilitated access to domain knowledge distilled from massive amounts of data





Future Work

- Promote broader use by experts, support evaluation
 - Insights to drive next-gen prompts, different types of Assistants
 - Refinement/automation of evaluation metrics
- Ontology extraction
 - Experiment with grounding on existing C2SIM ontology
 - Explore more robust ontology extraction techniques
 - LLM-based, e.g. Babaei Giglou, H., D'Souza, J., & Auer, S. (2023). LLMs4OL: Large Language Models for Ontology Learning. ArXiv, abs/2307.16648.
 - Mixing in traditional ontology learning techniques to handle sub-tasks
 - Few-shot learning
- Investigate fine-tuning techniques
 - Reinforcement learning from human feedback ?





Simulation Interoperability Standards Organization

"Simulation Interoperability & Reuse through Standards"

Related Materials on GitHub:

https://github.com/OpenC2SIM/C2SIMArtifacts/tree/main/Subgroups/ASX



EXTRA





Synthetic Scenario Generation

- Less of a risk of hallucinations for scenario generation as a development aid
 - Some level of "imagination" is not undesirable
 - Aim is to aid humans, which remain the final arbiters of the appropriateness of a scenario
- Current approach: Pipeline with multiple Assistants to offer opportunities for user tweaking
 - Scenarios from Objectives + Context generating synthetic scenarios
 - Areas to identify clusters of domain knowledge represented in the model
 - Objectives from Areas model consensus on entailed objectives





Prompt: What are the main scenarios of use of autonomous or robotic systems in the military?

"Autonomous or robotic systems have become increasingly significant in military operations, providing capabilities that enhance mission effectiveness, reduce the risk to human life, and perform tasks that are either too complex, too tedious, or too dangerous for human personnel. Here are some of the main scenarios of use of such systems in the military:

- 1. **Surveillance and Reconnaissance** Robotic systems, especially drones and unmanned aerial vehicles (UAVs), are widely used for surveillance and reconnaissance missions. They can cover vast areas, providing real-time data and imagery without exposing human operators to danger. This capability is vital for gathering intelligence, monitoring enemy movements, and assessing battlefield conditions.
- 2. **Explosive Ordnance Disposal (EOD)** Robots are extensively used for identifying, defusing, or safely detonating explosive devices and mines. EOD robots can navigate hazardous areas, reducing the risk to military personnel. These robots come equipped with cameras, sensors, and tools necessary for bomb disposal tasks.
- 3. **Logistics and Transport** Autonomous ground vehicles are being developed and used for logistical support, such as transporting supplies, equipment, and even wounded soldiers in and out of combat zones. These vehicles can operate in challenging terrains and environments, ensuring that human troops are well-supplied with reduced risk.
- 4. **Combat Operations** Though the use of fully autonomous lethal weapons is a subject of ethical and legal debate, there are semi-autonomous systems designed to support combat operations. These include unmanned ground vehicles (UGVs) and drones armed with weapons. These systems can provide support to human soldiers or serve as initial strike options where sending humans is too risky.
- 5. **Search and Rescue** In disaster zones or challenging terrains, robots and drones can be invaluable in searching for survivors, delivering emergency supplies, or assessing the damage. These systems can operate in environments that might be inaccessible or too dangerous for humans.
- 6. **Electronic Warfare (EW)** Autonomous systems are being used to conduct electronic warfare, including jamming enemy communications, deploying decoys to confuse enemy sensors, and protecting friendly forces from electronic attacks. The autonomy in these systems allows for rapid response to the dynamic EW environment.
- 7. **Communication Relays** In environments where traditional communication systems may be compromised, unmanned systems can serve as mobile communication relays, ensuring that units remain in contact. UAVs can be particularly effective in extending the range of communications in remote or challenging terrains.
- 8. **Medical Evacuation and Assistance** Autonomous systems are being explored for their potential to carry out medical evacuations or even provide frontline medical assessments and assistance. This could range from autonomous vehicles evacuating the wounded to robotic systems providing preliminary medical care.

These scenarios highlight the diverse applications of autonomous and robotic systems in the military. While their use promises enhanced operational capabilities and reduced risk to human life, it also presents challenges, including ethical considerations, reliability issues, and the need for robust command and control systems to manage these advanced technologies."





Force model to

reason about the

results

Prompt-enhancing meta-prompt

Assistant's role **Persona**: You are an expert in crafting highly efficient GPTdescription 4 prompts. **Input**: The user will provide a prompt to improve within Aid in interpreting square brackets ([]) input: use of markers to identify segments of interest **Procedure**: Using the guidelines in the attached document. identify opportunities for improvement. List all these opportunities, explaining which part of the attachment Grounding on document can be used to improve each. document: OpenAl's own **Output**: Improve the user provided prompt according to the instructions opportunities identified. Use the Attached copy of https://platform.openai.com/docs/guides/prompt- reasoning to engineering shape the output





Running it through itself...

GPT-4:

Based on my review of the strategies and tactics for improving prompt engineering as outlined in the document, here are the identified opportunities for enhancement regarding the userprovided prompt structure:

- Specifying the Persona Clearly: The prompt designates a specific persona for the Al. This aligns with the tactic to "ask the model to adopt a persona" for more tailored and contextually appropriate responses. Making the persona clear and detailed can help in crafting responses that meet specific requirements and expectations.
- 2. Detailed Instructions: The prompt specifies steps under "Procedure" for analyzing user prompts and improving them. This adheres to the idea of "writing clear instructions" and "specifying steps required to complete a task," which ensures that the task at hand is understood and executed efficiently.
- Suggesting Experimentation and Flexibility: The
 prompt encourages identifying opportunities for
 improvement and experimenting with those, reflecting
 the guideline to encourage experimentation to find
 methods that work best.

Improvements based on identified opportunities:

Persona: You are a master in optimizing GPT-4 prompts to elevate their efficiency and effectiveness. Your *expertise lies in identifying nuances that refine prompts, ensuring maximum clarity and precision...*

Input: Users will provide a prompt enclosed within square brackets ([]). Your role includes dissecting this prompt to pinpoint areas for enhancement.

Procedure:

- 1. Analyze the provided prompt comprehensively, drawing on advanced GPT-4 prompt engineering strategies.
- 2. Identify explicit and nuanced opportunities for refinement. Use your extensive knowledge to explain how each part of the prompt can be improved, referencing relevant prompt engineering techniques.
- 3. Leverage your deep understanding of GPT models, especially GPT-4, to tailor improvements. Ensure that your suggestions enhance clarity, precision, and the ability to generate high-quality, contextually appropriate responses.
- 4. Experiment with different enhancements to discover the most effective strategies for the specific case at hand.

Output: Craft a revised version of the user's prompt, incorporating the identified improvements. Ensure the new prompt is succinct, clear, and structured to guide GPT-4 in generating insightful, precise responses.





Ultimately...



Identify techniques and tools to quickly/automatically extract ontologies from new domains in general

Authoritative & Synthetic documents + LLM → domain ontology



To automate the generation of natural language interfaces

Ontology logical forms + descriptive language from documents → NL UI

- Transformation of natural language statements into formal machine-processable representations
- Natural language question answering in the domain



Example: Sketch-Thru-Plan Speech and Sketch input generating C2SIM SMX+LOX (+ASX)

- Natural language input of APP6/2525 Courses of Action
- Currently:
 - SME crafted input language, enriched with LLM-generated glosses
 - Rendered as C2SIM Executable by Simulators, exportable to compliant C2
- Future: shorter, automation-supported UI generation

