

Autonomous Industrial Control using an Agentic Framework with Large Language Models

Javal Vyas, Mehmet Mercangöz

*Autonomous Industrial Systems Lab, Imperial College London,
Imperial College Rd, South Kensington Campus, London, SW7 2AZ,
United Kingdom*

Abstract: As chemical plants evolve towards full autonomy, the need for effective fault handling and control in dynamic, unpredictable environments becomes increasingly critical. This paper proposes an innovative approach to industrial automation, introducing validation and reprompting architectures utilizing large language model (LLM)-based autonomous control agents. The proposed agentic system—comprising of operator, validator, and reprompter agents—enables autonomous management of control tasks, adapting to unforeseen disturbances without human intervention. By utilizing validation and reprompting architectures, the framework allows agents to recover from errors and continuously improve decision-making in real-time industrial scenarios. We hypothesize that this mechanism will enhance performance and reliability across a variety of LLMs, offering a path toward fully autonomous systems capable of handling unexpected challenges, paving the way for robust, adaptive control in complex industrial environments. To demonstrate the concept's effectiveness, we created a simple case study involving a temperature control experiment embedded on a microcontroller device, validating the proposed approach.

Keywords: Autonomous systems, industrial AI, generative AI, multi-agent systems.

1. INTRODUCTION

Chemical plants are moving towards autonomous operations. Especially for routine operations that follow well-defined procedures, autonomous operation is considered technically feasible with currently available technologies (Borghesan et al. (2022)). However, a significant challenge in developing autonomous control systems is the need to account for long-tail events, which are rare, unpredictable occurrences that fall outside of the scope of typical operational scenarios. In industrial contexts, these long-tail events can range from unexpected equipment failures to highly unusual process disturbances. Traditional automation approaches struggle to handle such events, as they rely heavily on predefined rules and algorithms, rendering them overly rigid and poorly adapted to situations that deviate from expected patterns. Solutions leveraging machine learning models have made some progress in handling known unknowns such as known disturbances or possible plant-model mismatch but they tend to fail in handling anomalies. This is primarily because these models are trained on majority-class data, as anomaly data is scarce or available in too few samples. As a result, these solutions struggle to detect and react to anomalies in real-time, particularly in scenarios involving unknown unknowns—unforeseen disturbances that the system was not designed to handle.

Currently, human operators play a key role in managing the type of unknown unknowns discussed previously. Leveraging their reasoning abilities and domain knowledge human operators can dynamically assess a situation and adjust their actions based on real-time feedback. The overarching goal of this work is to bridge these reasoning and knowledge use abilities to autonomous systems using generative machine learning models as intelligent control agents. We particularly focus on the use of Large Language Models (LLMs) for this purpose.

LLMs, with their extensive knowledge bases and reasoning capabilities, represent a promising avenue for developing intelligent control agents capable of autonomously analyzing incoming data, diagnosing anomalies, and making informed control decisions in a zero-shot manner—making inferences and offering solutions to scenarios they have not explicitly encountered in training (Pantelides et al., 2024). The challenge is transitioning to a fully automated system that can evaluate responses and adjust actions independently. To address this, we propose a reprompting architecture that empowers LLMs to function as autonomous control agents. This architecture enables agents to validate their actions against a digital twin, implementing them in the physical system if they pass validation; if not, the agent is prompted to revise its approach. This iterative process significantly enhances decision-making capabilities and improves system performance in real-time.

* The authors gratefully acknowledge the financial support provided by the Department of Chemical Engineering at Imperial College London for this work

2. RELATED WORK

2.1 Evolution of Autonomous Systems for Industrial Control

Autonomous systems have been defined in various ways across the literature, with some emphasizing their capability to solve tasks independently of specific programming instructions (Hrabia et al. (2015), Abbass et al. (2018)) and others noting their ability to achieve goals without step-by-step guidance (Beer et al. (2014), Watson and Scheidt (2005)). Another perspective highlights autonomy as the capacity to make decisions under incomplete information (Abbass et al. (2018), Aniculaesei et al. (2018)). These definitions underscore the growing role of artificial intelligence (AI) in industrial control systems, positioning Autonomous Industrial Systems as a key area within Industrial AI, intersecting with fields like Machine Learning, Natural Language Processing, and Robotics (Peres et al. (2020)).

Initial approaches in agent based systems utilized rule-based agents for tasks such as intrusion detection (Jha and Hassan (2002)) or decision support (Gao et al. (2009)). Despite some success, rule-based agents are inherently limited to predefined situations, making them less adaptable to novel scenarios (Siu et al. (2021)). This constraint led researchers to explore machine learning and deep learning (DL) agents, which can adapt based on data. For instance, DL-based multi-agent systems have shown effectiveness in intrusion detection (Louati and Ktata (2020)), yet the complexities of data collection and validation in distributed environments create substantial challenges in many industrial applications (Hanga and Kovalchuk (2019)).

To address these limitations, researchers turned to reinforcement learning (RL) agents. RL agents, while highly effective for specialized tasks, face challenges in sample efficiency, generalizability, and lengthy training times (Cheng et al. (2024)). Despite their effectiveness in specific applications like process control in crystallization (Meng et al. (2023)) and inventory management (Mousa et al. (2024)), RL-based approaches often require well-defined problem settings and reward functions, which can limit their scalability in complex, dynamic environments (Nian et al. (2020)) and may not be well suited for handling anomalous conditions.

2.2 Large Language Models (LLMs) in Industrial Control

Recently, large language models (LLMs) have emerged as a promising tool in agent based systems due to their adaptability and generalization abilities. LLMs have made significant inroads in chemical engineering, such as predicting material properties (Jia et al. (2024), Balaji et al. (2023)) and process decision-making (Chen et al. (2024a), Schweidtmann (2024)). LLMs have also been employed for tasks like fault detection and flowsheet generation, where they assist in complex problem-solving by completing, correcting, or even generating flowsheets autonomously (Balhorn et al. (2024), Hirtreiter et al. (2023)).

LLMs have also been considered for industrial control as well. Song et al. (2023) proposed a framework to control the HVAC system in a building using an LLM. Researchers

used the historical demonstrations along with the prompt to the LLM performance in controlling the HVAC system in the building. They demonstrated that an LLM performs equivalent or surpasses the RL performance. Researchers have also used LLMs for the modular production and control of autonomous industrial systems, where the LLMs are connected to the digital twins and LLMs adapt with the interactions with the digital twin for a specific task (Xia et al. (2023)). Xia et al. (2024) propose a framework to achieve an end to end industrial automation system. Their framework supplies LLMs with real-time events on different context semantic levels, allowing them to interpret the information, generate production plans, and control operations on the automation system. In this work, the researchers propose to use a digital-twin of the industrial system for generating context for the automation agents but they do not consider a validation or reprompting scheme or the generation of any kind of feedback or critique for the LLM actions.

2.3 Prompting Strategies for Enhanced Control

Prompting strategies have become central to improving LLMs' decision-making abilities in complex tasks. Among these, the Chain of Thought (CoT) approach prompts LLMs to break down tasks into intermediate reasoning steps before producing a final response (Wei et al. (2022)). Building on this, the Tree of Thought (ToT) approach expands on CoT by allowing LLMs to explore multiple paths in their reasoning (Yao et al. (2023)), and the Graph of Thought (GoT) consolidates LLM reasoning paths to enhance task completion accuracy (Besta et al. (2024)).

Other prompting frameworks adapt feedback-driven approaches to improve LLM behavior in agent-based settings. REACT (Yao et al. (2022)) enables agents to process thoughts before taking actions, while REFLECTION (Shinn et al. (2023)) allows agents to interact with the system, reflect on actions, and store the interaction history for iterative learning. Related approaches, including self-refine (Madaan et al. (2023)), RCI (Kim et al. (2023)), and self-debugging (Chen et al. (2023)), utilize feedback for error-correction and optimization in domain-specific tasks. For iterative tasks, Chen et al. (2024b) introduce a "gradient descent" style reprompting method to refine prompts based on interaction history, while Xu et al. (2024) use automatic reprompting with CoT to improve task accuracy.

This progression toward LLMs highlights their potential to address the limitations of earlier methods, providing a versatile approach that combines interpretability and robustness for industrial automation.

2.4 Contribution

In this work, we introduce the concept of using reprompting architectures for industrial control, where LLMs operate autonomously in complex process environments. The idea here is to have an agent based system which can carry out tasks autonomously. The engine for the agents in the system would be a large language model (LLM). We hypothesize that with the reprompting architecture, the performance of the system would improve. LLMs which

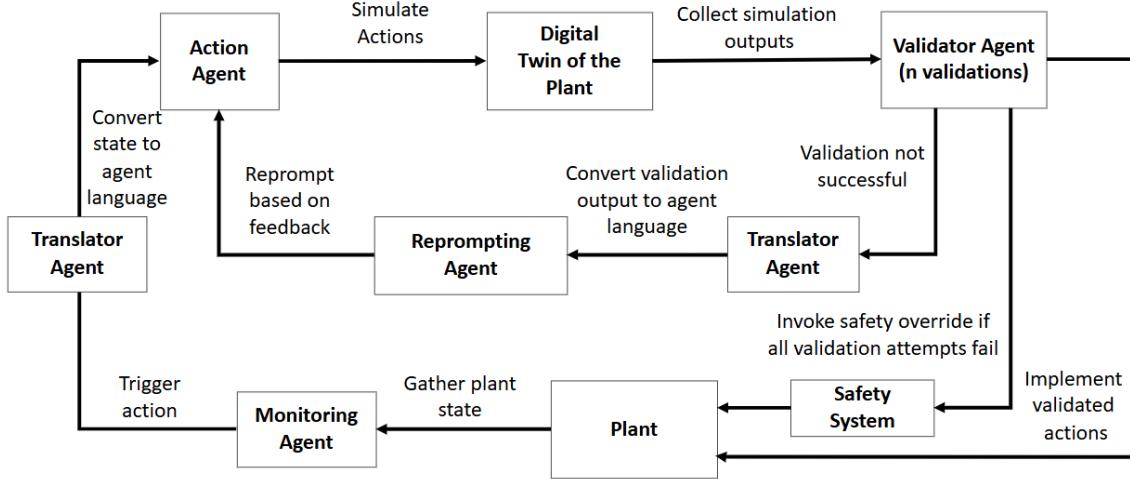


Fig. 1. Schematic of an agentic framework for monitoring and controlling a process plant during anomalous conditions

are prone to hallucinations as their inherent model characteristic may result in erroneous action, which can be hazardous in safety critical systems. Thus, having another agent which acts as a critique in navigating to an safe-to-optimal response would decrease the likelihood of the error rates. More specifically we introduce validation agents utilizing a simulation capability e.g. using a digital-twin to check the utility of the actions generated by the LLM agents and use a reprompting agent to provide feedback to the actor agent for improving the action in case the previously suggested action does not pass the validation check.

To illustrate the potential of this approach, we present a case study focused on temperature control using a physical micro-controller. We argue that this methodology aligns with the growing trend towards adaptive, fully autonomous systems and establishes a new pathway for intelligent industrial automation.

The following sections delve deeper into the components of the proposed framework. Section 3 provides an overview of the framework and its components. In section 4 we present the temperature control case study and its architecture. Section 5 discusses the results of the case study and its findings. Finally, section 6 we touch upon the future work.

3. METHODOLOGY

The proposed framework introduces a modular and adaptive LLM-based multi-agent system, with a focus on programmatically leveraging a Reprompting step via a Reprompter Agent to guide an Actor Agent toward safe and effective solutions. Each agent is assigned a specific role, equipped with tools, and tasked with distinct actions that contribute to the overarching system objectives. This section outlines the framework's role in enhancing system reliability and responsiveness through a coordinated agent-based approach.

3.1 Framework Overview

The core of this framework is built around four principal agents—the Monitoring Agent, Actor Agent, Validator

Agent, and Reprompter Agent—that interact with a simulated digital twin environment (see e.g. Fig 1). This digital twin serves as a proxy for the physical system, enabling safe validation of actions and structured feedback loops before passing actions to the physical plant.

- **Monitor Agent:** The Monitoring Agent gathers the state from the plant and can act as a versatile agent. The Monitoring agent can be used for both continuous control or anomaly detection. In case of continuous control, it would keep the track of the performance of the system and would allow for a planned action in a continuous manner. While in case of anomaly detection, the Monitoring agent would only trigger the subsequent agents if it detects the anomaly.
- **Actor Agent:** The Actor Agent initiates actions aimed at achieving control objectives, such as modifying parameters or toggling operational states. It operates based on predefined goals, and once it formulates an action, the Actor Agent passes this decision to the digital twin. This simulation evaluates the potential effects of the action, minimizing the risk of unsafe interventions on the physical system.
- **Digital Twin Simulation:** The digital twin emulates the behavior of the physical system in response to the Actor Agent's actions, enabling real-time assessment in a no-risk environment. This simulated feedback captures anticipated system responses, allowing agents to test actions safely before deployment.
- **Validator Agent:** Following the simulation, the Validator Agent assesses the Actor Agent's proposed action based on safety and operational criteria. If the action meets these criteria, it is ready for physical deployment. However, if it is deemed unsafe or suboptimal, the Validator Agent flags the action, prompting the Reprompter Agent to intervene for a predefined iterations after which, if the actions are unsafe, the safety system would override the actions.
- **Reprompter Agent:** The Reprompter Agent is a pivotal component in ensuring system safety and refinement. When an action fails validation, the Reprompter Agent collaborates with the Actor Agent to

adjust the initial decision. Using alternative prompts generated by processing the digital-twin outputs, the Reprompter Agent conditions the Action Agent until it aligns with the Validator Agent's criteria. This process forms a feedback loop in which each iteration is tested in the digital twin and validated again, ensuring the action is both safe and optimized. The loop persists until the action either satisfies validation standards or reaches a predefined limit on iterations, safeguarding stability in the control process.

This structured interaction between agents, anchored by the Reprompter Agent's corrective capabilities, enables the system to autonomously navigate complex control environments. By leveraging programmatic refinement, the Reprompter Agent helps the Actor Agent reach safe and effective solutions, ensuring robust and adaptive control in dynamic industrial settings.

3.2 Components of framework

- **Agents:** Each agent functions as a specialized LLM-driven entity with a distinct role in the feedback loop, contributing to adaptive control:
 - **Role:** Defines the purpose of each agent.
 - **Goal:** Provides clarity on what each agent should achieve.
 - **LLM:** Serves as the core reasoning engine, enabling agents to analyze, evaluate, and adapt.
 - **Tools:** Specify tools which the agent would have access to in the decision making process.
- **Tools:** These serve as specialized utility functions that support agents during decision-making. Tools enable agents to handle tasks that are beyond the core capabilities of an LLM, such as performing complex calculations or accessing specific lookup tables. By supplementing the LLM's reasoning with precise computational and data-access functions, the tools enhance the agents' ability to make informed, accurate decisions.
- **Tasks:** These are targeted assignments given to each agent, ranging from concise directives to detailed instructions that guide the LLM in executing specific actions. Tasks are carefully assigned to agents equipped with the necessary expertise or context, ensuring the agent's background aligns with the requirements of the task. Each task description provides clear guidance to optimize agent performance and streamline the overall decision-making process.

In summary, this methodology outlines a structured, iterative framework designed to leverage the capabilities of Large Language Model (LLM)-based agents in autonomous industrial control. Each component, from specialized agents to supporting tools and defined tasks, works in concert to ensure safe, adaptive, and effective control actions within a digital twin environment. The introduction of a Reprompter Agent strengthens the system's resilience, facilitating a feedback-driven refinement process that iteratively adjusts actions until they meet safety and efficacy standards.

To demonstrate the practical application of this framework, we present a case study in temperature regulation. This case study illustrates the roles and interactions of

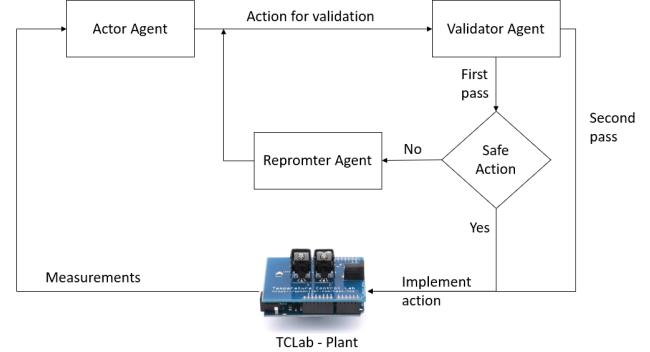


Fig. 2. Case Study Schematic

the Actor, Validator, and Reprompter agents in real-world scenarios, showcasing the framework's capability to autonomously navigate complex control challenges.

4. CASE STUDY

This case study demonstrates the application of the proposed LLM-based multi-agent framework to autonomously control a physical Arduino microcontroller known as TCLab (Oliveira and Hedengren (2019)). The setup aims to manage heater operations based on specific temperature thresholds: heaters are turned off when the temperature exceeds 27°C and turned on when it falls below 25°C. This creates a cyclical oscillation within these thresholds, with the control sequence monitored over a 40-minute period. The goal of this case study is to assess how effectively the proposed multi-agent framework improves via the use of re-prompting for autonomous control under real-world conditions.

Structure of the Case Study The case study employs a three-agent structure (Fig 2), each with distinct roles to facilitate intelligent decision-making and control processes:

- **Operator Agent:** The Operator agent initiates an action based on real-time temperature readings. It determines when to activate or deactivate the heater based on the predefined thresholds(4). By leveraging its role-specific prompts (3), the Operator Agent interprets data and issues commands to maintain the target temperature range.
- **Validator Agent:** The Validator Agent assesses the actions proposed by the Operator Agent. It verifies whether the action aligns with the control logic—specifically, maintaining temperatures within the desired range. If the proposed action does not meet the criteria, the Validator flags it for reevaluation, preventing potentially unsafe or incorrect responses from being implemented.
- **Reprompter Agent:** Upon a validation failure, the Reprompter Agent is activated to analyze and refine the action suggested by the Operator Agent. The Reprompter Agent recalibrates the initial action to ensure it aligns with the system's predefined requirements. The refined action undergoes a secondary validation before being deployed.

While the framework is generally designed to work with a digital twin model, the simplicity of this control task allows

```

Role = Plant Operator,
Goal = Operate the heating process within the desirable limits,
Backstory = You have expert knowledge about process control and expertise in finite state
machines and relay switches,
Tools = [],
Verbose = True,
Llm = llm

```

Fig. 3. Operator Agent Description

```

description=Task: Operate the system between {lo_temp}°C and {hi_temp}°C.
Description: The system can only operate in two modes:
a. Heating mode: Encoded as 1 (active heating).
b. Cooling mode: Encoded as 0 (no active heating).
The system should be operated using the following constraints.
1. Heat the system until the temperature reaches {hi_temp}°C (upper threshold)
by switching to heating mode.
2. Stop heating once the temperature strictly crosses {hi_temp}°C, allowing it to
cool by switching to a cooling mode.
3. The system must wait until the temperature strictly drops below {lo_temp}°C
(lower threshold) before resuming heating using the heating mode.
Output: A single integer (1 for heating, 0 for cooling), based on the current
temperature relative to the thresholds.
**Parameters**:
- Curr_state: (curr_state),
- Curr_temp: (curr_temp),
- lo_temp: {lo_temp},
- hi_temp: {hi_temp}
Note: Strictly only output the next state, as more outputs are costly for the LLMs.
),
agent=agent,
expected_output = 'A single integer indicating the next state'

```

Fig. 4. Operator Agent Task Description

us to embed it into the Validator Agent in this case study. This approach demonstrates the framework's adaptability to different control tasks, highlighting each agent's contribution to maintaining stable, autonomous control. Future work will integrate a digital twin, particularly for complex, safety-critical scenarios like fault detection, enhancing the framework's robustness for advanced industrial control. This case study underscores the potential of this multi-agent configuration to autonomously manage and correct actions in real-world applications.

5. RESULTS

The case study framework was realized using CrewAI multi-agent platform (CrewAI, 2024). The framework was created and executed locally while the agents' engine utilized LLMs from OpenAI suite (OpenAI, 2024) accessed in the cloud via the OpenAI APIs for the corresponding LLMs. The communication between TCLab and the framework was achieved via a Python based wrapper. The performance of the proposed framework, leveraging OpenAI's large language models (LLMs) suite as control agents, was evaluated within a temperature regulation case study. This evaluation centered on the agents' accuracy in executing control actions and their control performance. We measured accuracy across two settings—initial pass accuracy and accuracy post-reprompting—to analyze the models' ability to correct missteps autonomously.

Table 1. Accuracy Performance of Language Models in the proposed framework

Metric	GPT3.5	GPT4omini	GPT4o	GPT4
Accuracy- first pass (%)	60.04	72.49	99.63	93.75
Accuracy - reprompts (%)	85.34	89.97	99.81	96.09
Samples	423	394	554	128
Passes	254	253	552	120
Fails	169	61	2	8
Pass after reprompts	107	96	1	3

The results in Table 1 show a two fold story, one is about the sampling rates and other about the accuracy.

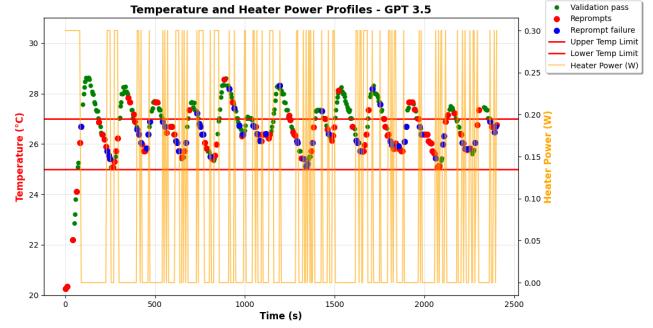


Fig. 5. Temperature Profile for GPT 3.5

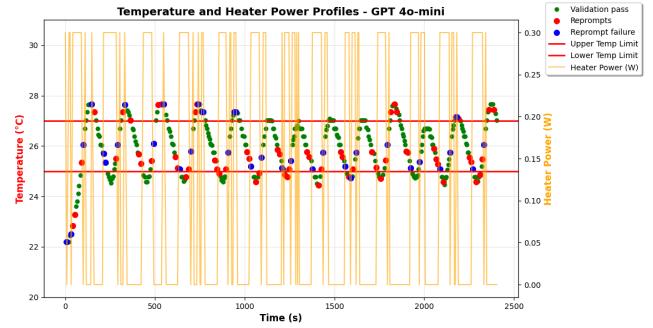


Fig. 6. Temperature Profile for GPT 4o-mini

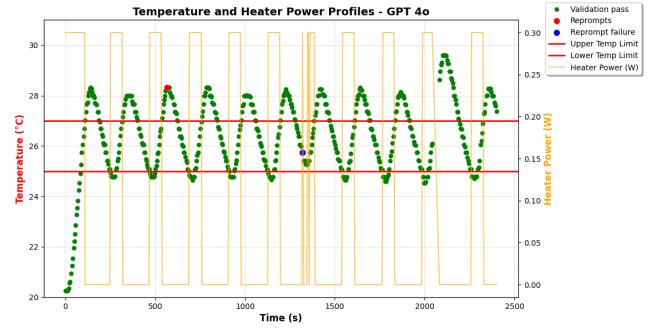


Fig. 7. Temperature Profile for GPT 4o

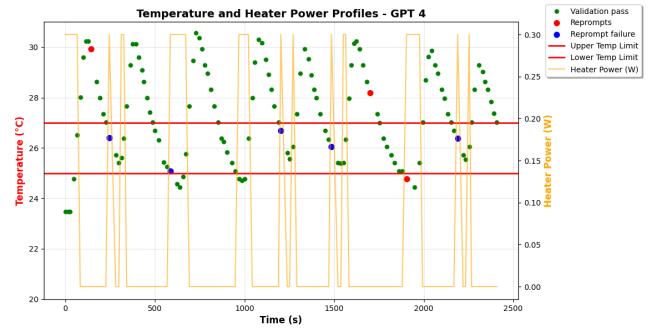


Fig. 8. Temperature Profile for GPT 4

Here the sampling rates for GPT 4o is the highest while GPT 4 has the lowest sampling rate. This is a result of the inference time of these models, thus impact the sampling rates. This although of lesser importance for this application, indicates that autonomous systems with LLM based agents may not be suitable for a system that needs to have fast dynamics.

In terms of accuracy, GPT 4o outperforms other OpenAI models, with GPT 4 following as the second-best performer. Notably, when reprompting is applied, the system's performance increases across all models, with the most significant improvement observed in GPT 3.5 rising from 60.4% to 85.34%. These results highlight the potential of reprompting architectures to enhance model performance significantly, enabling even less capable models to approach the accuracy of more advanced ones.

The control performance of these models were evaluated using the average temperate deviation from the midpoint of the temperature range. Table 2 shows that GPT 4o mini has the best control performance where the overshoots and undershoots are minimal, whereas while GPT 4 being highly accurate performs the worst in control performance amongst the OpenAI LLM suite. This is attributed to the inference time of the model. For GPT 4 the inference time was high resulting in previous action being implemented for an extended period of time. Since the system does not have cooling, even when the heaters are switched off, residual heat continues to dissipate, raising the temperature further. Thus, it is important to note that LLM inference times do influence the control performance of the system.

Table 2. Control Performance of Language Models in the proposed framework

Metric	GPT3.5	GPT4omini	GPT4o	GPT4
Average Deviation	0.832	0.077	0.582	1.469
Time above 27C (s)	949	499.10	887.70	1163.09
Time below 25C (s)	0	432.30	285.87	173.40
Time outside range (s)	949.24	931.40	1173.58	1336.50

These results confirm that the proposed framework effectively utilizes LLMs as control agents, and the reprompting mechanism significantly enhances accuracy and reliability, especially for models with initially lower performance.

6. CONCLUSION

In conclusion, this paper highlights the promising potential of large language models (LLMs) as autonomous control agents in industrial applications. The proposed framework, enhanced by a reprompting architecture, demonstrates a significant capability for agents to autonomously correct their actions, leading to improved reliability and accuracy in control tasks. Our results indicate that even earlier models like GPT 3.5-turbo can achieve substantial performance gains through reprompting, with accuracy improving from 60.04% to 85.34%. More advanced models, such as GPT 4o, reached near-perfect accuracy exceeding 99%, showcasing the framework's effectiveness in harnessing LLMs for control tasks with proposed framework.

These findings validate the viability of LLM-based systems in autonomous industrial control, where rapid and precise decision-making is essential. While this case study focused on a relatively straightforward task, the adaptability of the framework positions it well for application in more complex control scenarios. Future work may explore its deployment in fault handling and digital twin environments, where real-time decision-making is critical in dynamic and unpredictable settings. Overall, this research supports the integration of LLMs with reprompting architecture as a vital component toward realizing fully autonomous and intelligent industrial systems.

REFERENCES

- Abbass, H.A., Scholz, J., and Reid, D.J. (2018). *Foundations of trusted autonomy*. Springer Nature.
- Aniculaesei, A., Grieser, J., Rausch, A., Rehfeldt, K., and Warnecke, T. (2018). Towards a holistic software systems engineering approach for dependable autonomous systems. In *Proceedings of the 1st International Workshop on Software Engineering for AI in Autonomous Systems*, 23–30.
- Balaji, S., Magar, R., Jadhav, Y., and Farimani, A.B. (2023). Gpt-molberta: Gpt molecular features language model for molecular property prediction.
- Balhorn, L.S., Caballero, M., and Schweidtmann, A.M. (2024). *Toward autocorrection of chemical process flow-sheets using large language models*, 3109–3114. Elsevier. doi:10.1016/b978-0-443-28824-1.50519-6.
- Beer, J.M., Fisk, A.D., and Rogers, W.A. (2014). Toward a framework for levels of robot autonomy in human-robot interaction. *Journal of human-robot interaction*, 3(2), 74.
- Besta, M., Blach, N., Kubicek, A., Gerstenberger, R., Podstawski, M., Gianinazzi, L., Gajda, J., Lehmann, T., Niewiadomski, H., Nyczek, P., and Hoefler, T. (2024). Graph of thoughts: Solving elaborate problems with large language models. *Proceedings of the AAAI Conference on Artificial Intelligence*, 38(16), 17682–17690. doi:10.1609/aaai.v38i16.29720.
- Borghesan, F., Zagorowska, M., and Mercangöz, M. (2022). Unmanned and autonomous systems: Future of automation in process and energy industries. *IFAC-PapersOnLine*, 55(7), 875–882.
- Chen, H., Constante-Flores, G.E., and Li, C. (2024a). Diagnosing infeasible optimization problems using large language models. *INFOR: Information Systems and Operational Research*, 1–15.
- Chen, W., Koenig, S., and Dilkina, B. (2024b). Reprompt: Planning by automatic prompt engineering for large language models agents. doi:10.48550/ARXIV.2406.11132.
- Chen, X., Lin, M., Schärli, N., and Zhou, D. (2023). Teaching large language models to self-debug. doi:10.48550/ARXIV.2304.05128.
- Cheng, Y., Zhang, C., Zhang, Z., Meng, X., Hong, S., Li, W., Wang, Z., Wang, Z., Yin, F., Zhao, J., and He, X. (2024). Exploring large language model based intelligent agents: Definitions, methods, and prospects. doi:10.48550/ARXIV.2401.03428.
- CrewAI (2024). Crewai: An autonomous control framework. URL <https://github.com/crewai/crewai>. Accessed: 2024-11-08.
- Gao, Y., Shang, Z., and Kokossis, A. (2009). Agent-based intelligent system development for decision support in chemical process industry. *Expert Systems with Applications*, 36(8), 11099–11107. doi:10.1016/j.eswa.2009.02.078.
- Hanga, K.M. and Kovalchuk, Y. (2019). Machine learning and multi-agent systems in oil and gas industry applications: A survey. *Computer Science Review*, 34, 100191.
- Hirtreiter, E., Schulze Balhorn, L., and Schweidtmann, A.M. (2023). Toward automatic generation of control structures for process flow diagrams with large language models. *AIChE Journal*, 70(1). doi:10.1002/aic.18259.
- Hrabia, C.E., Masuch, N., and Albayrak, S. (2015). A metrics framework for quantifying autonomy in com-

- plex systems. In *Multiagent System Technologies: 13th German Conference, MATES 2015, Cottbus, Germany, September 28-30, 2015, Revised Selected Papers* 13, 22–41. Springer.
- Jha, S. and Hassan, M. (2002). Building agents for rule-based intrusion detection system. *Computer Communications*, 25(15), 1366–1373. doi:10.1016/s0140-3664(02)00038-5.
- Jia, S., Zhang, C., and Fung, V. (2024). Llmatdesign: Autonomous materials discovery with large language models.
- Kim, G., Baldi, P., and McAleer, S. (2023). Language models can solve computer tasks. In *Advances in Neural Information Processing Systems*, volume 36, 39648–39677. Curran Associates, Inc.
- Louati, F. and Ktata, F.B. (2020). A deep learning-based multi-agent system for intrusion detection. *SN Applied Sciences*, 2(4), 675.
- Madaan, A., Tandon, N., Gupta, P., Hallinan, S., Gao, L., Wiegreffe, S., Alon, U., Dziri, N., Prabhumoye, S., Yang, Y., Gupta, S., Majumder, B.P., Hermann, K., Welleck, S., Yazdanbakhsh, A., and Clark, P. (2023). Self-refine: Iterative refinement with self-feedback. doi:10.48550/ARXIV.2303.17651. URL <https://arxiv.org/abs/2303.17651>.
- Meng, Q., Anandan, P.D., Rielly, C.D., and Benyahia, B. (2023). *Multi-Agent Reinforcement Learning and RL-Based Adaptive PID Control of Crystallization Processes*, 1667–1672. Elsevier. doi:10.1016/b978-0-443-15274-0.50265-1.
- Mousa, M., van de Berg, D., Kotecha, N., del Rio Chanona, E.A., and Mowbray, M. (2024). An analysis of multi-agent reinforcement learning for decentralized inventory control systems. *Computers and Chemical Engineering*, 188, 108783. doi:10.1016/j.compchemeng.2024.108783.
- Nian, R., Liu, J., and Huang, B. (2020). A review on reinforcement learning: Introduction and applications in industrial process control. *Computers and Chemical Engineering*, 139, 106886. doi:10.1016/j.compchemeng.2020.106886.
- Oliveira, P.M. and Hedengren, J.D. (2019). An apmonitor temperature lab pid control experiment for undergraduate students. In *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 790–797. IEEE.
- OpenAI (2024). Gpt-3.5, gpt-4, or other openai models. URL <https://openai.com>. Accessed: 2024-11-08.
- Pantelides, C., Baldea, M., Georgiou, A.T., Gopaluni, B., Mehmet, M., Sheth, K., Zavala, V.M., and Georgakis, C. (2024). From automated to autonomous process operations. doi:10.2139/ssrn.4963632.
- Peres, R.S., Jia, X., Lee, J., Sun, K., Colombo, A.W., and Barata, J. (2020). Industrial artificial intelligence in industry 4.0 - systematic review, challenges and outlook. *IEEE Access*, 8, 220121–220139. doi:10.1109/ACCESS.2020.3042874.
- Schweidtmann, A.M. (2024). Generative artificial intelligence in chemical engineering. *Nature Chemical Engineering*, 1(3), 193–193. doi:10.1038/s44286-024-00041-5.
- Shinn, N., Cassano, F., Berman, E., Gopinath, A., Narasimhan, K., and Yao, S. (2023). Reflexion: Language agents with verbal reinforcement learning. doi:10.48550/ARXIV.2303.11366.
- Siu, H.C., Peña, J., Chen, E., Zhou, Y., Lopez, V., Palko, K., Chang, K., and Allen, R. (2021). Evaluation of human-ai teams for learned and rule-based agents in hanabi. In *Advances in Neural Information Processing Systems*, volume 34, 16183–16195. Curran Associates, Inc.
- Song, L., Zhang, C., Zhao, L., and Bian, J. (2023). Pre-trained large language models for industrial control. doi:10.48550/ARXIV.2308.03028.
- Watson, D.P. and Scheidt, D.H. (2005). Autonomous systems. *Johns Hopkins APL technical digest*, 26(4), 368–376.
- Wei, J., Wang, X., Schuurmans, D., Bosma, M., Ichter, B., Xia, F., Chi, E., Le, Q., and Zhou, D. (2022). Chain-of-thought prompting elicits reasoning in large language models. doi:10.48550/ARXIV.2201.11903.
- Xia, Y., Jazdi, N., Zhang, J., Shah, C., and Weyrich, M. (2024). Control industrial automation system with large language models. doi:10.48550/ARXIV.2409.18009.
- Xia, Y., Shenoy, M., Jazdi, N., and Weyrich, M. (2023). Towards autonomous system: flexible modular production system enhanced with large language model agents. In *2023 IEEE 28th International Conference on Emerging Technologies and Factory Automation (ETFA)*, 1–8. doi:10.1109/ETFA54631.2023.10275362.
- Xu, W., Banburski, A., and Jovic, N. (2024). Reprompting: Automated chain-of-thought prompt inference through gibbs sampling.
- Yao, S., Yu, D., Zhao, J., Shafran, I., Griffiths, T.L., Cao, Y., and Narasimhan, K. (2023). Tree of thoughts: Deliberate problem solving with large language models. doi:10.48550/ARXIV.2305.10601.
- Yao, S., Zhao, J., Yu, D., Du, N., Shafran, I., Narasimhan, K., and Cao, Y. (2022). React: Synergizing reasoning and acting in language models. doi:10.48550/ARXIV.2210.03629.