Deterministic Safety of AI Agent-Embodied Robots Using a Model-Based Design Approach and Lingua Franca Open-source Framework for Cyber-Physical Systems

Lingua Franca Website

Daniel Fan, Electrical Engineering Major
Mentors: Dr. Hokeun Kim, Assistant Professor and Deeksha Prahlad, PhD Student
School of Computing and Augmented Intelligence

GitHub Repository

Objective and Research Question

The goal of this project is to design a framework that can enforce deterministic and time-predictable safety behavior in AI-powered robotic agents operating within safety-critical cyber-physical systems (CPS).

Background

- AI-powered robots deployed in safety-critical environments, introduce non-determinism due to LLM agents, human-in-the-loop (HITL) and dynamic environment.
- Reactor model of computation enables determinism, time-coordinated, event-driven execution.
- Lingua Franca (LF), an open-source coordination language.
- MuJoCo enables high fidelity physics-based testing and validation.

Experimental Setup

- GPU: NVIDIA RTX 6000 Blackwell Pro
- CPU: Intel Xeon w9-3475X
- Memory: 256 GB DDR5 RAM
- LLM: 4-bit quantized Llama 3 (8B)

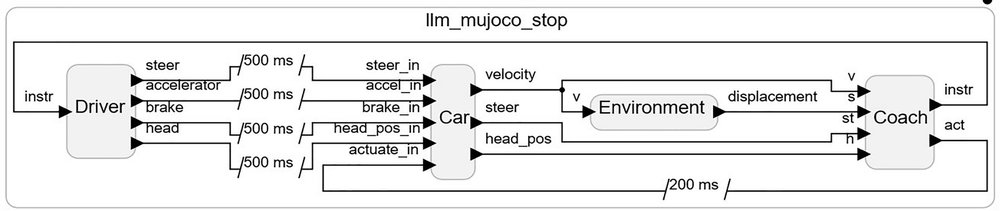


Figure 1: Proposed reactor model implemented in LF

Proposed Approach

- Adopt a reactor-based model, implemented in Lingua Franca (LF), to enforce deterministic execution.
- Deterministic modeling of agentic coach as HITL-CPS

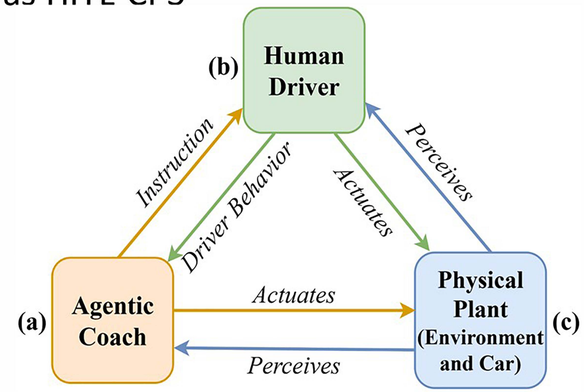


Figure 2: HITL CPS depicted interactions

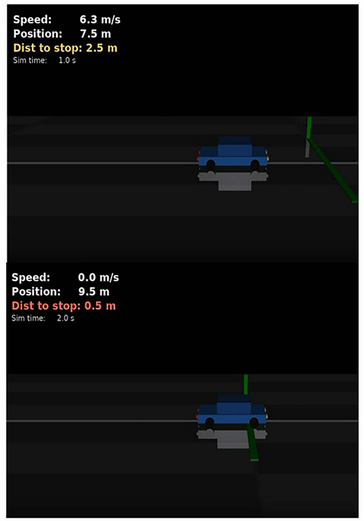
- Agentic driving coach issues instructions to the driver based on the accelerator, brake, steer, and head inputs.
- External safety fallback mechanism if the LLM-based coach fails to instruct on time
- MuJoCo simulation models vehicle position and speed in a physics-based environment

References

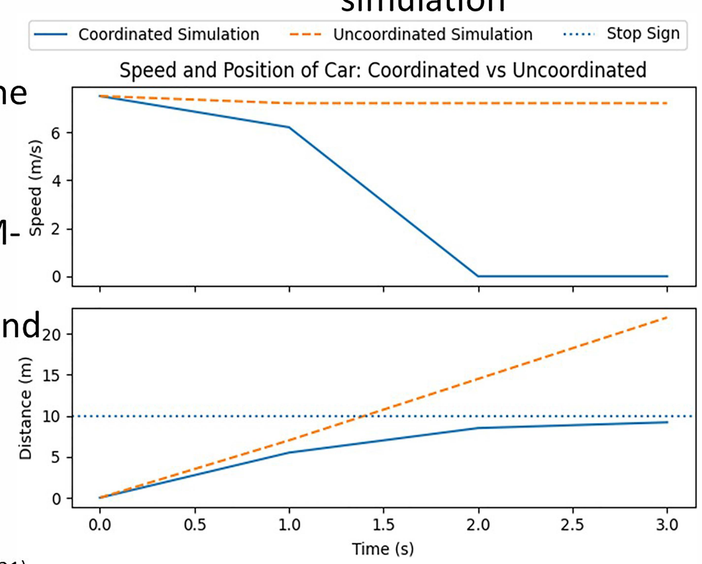
[1]Soroush Bateni et al. 2023. Risk and Mitigation of Nondeterminism in Distributed Cyber-Physical Systems. In Proceedings of the 21st ACM-IEEE International Conference on Formal Methods and Models for System Design (Hamburg, Germany)(MEMOCODE '23). ACM, 1–11
[2]Marten Lohstroh et al. 2021. Toward a Lingua Franca for Deterministic Concurrent Systems. ACM Trans. on Embedded Computing Syst. (TECS) 20, 4 (2021)

Results

(a) LF-based simulation



(b) uncoordinated simulation



FURI

ASU KIM KNOWLEDGEABLE & INTERACTIVE MACHINES

ASU Ira A. Fulton Schools of Engineering
Arizona State University