

High Performance High-Assurance Interval Arithmetic Based Safety Monitoring for Robot Arms on Industrial Multi-Core PLCs



José Cestero, John Rogan, Franz Franchetti | Carnegie Mellon University
Tao Cui | Siemens U.S.

Overview

Problem: Floating-Point PLC Arithmetic

- Programmable Logic Controllers (PLCs) excel at safety-guaranteed ladder logic, yet fall short when it comes to safe floating-point computation
- Use cases are severely limited due to the fact, and complex arithmetic is unfeasible to run on PLC hardware

PLC Hardware

PLC Diagram



RIB Diagram

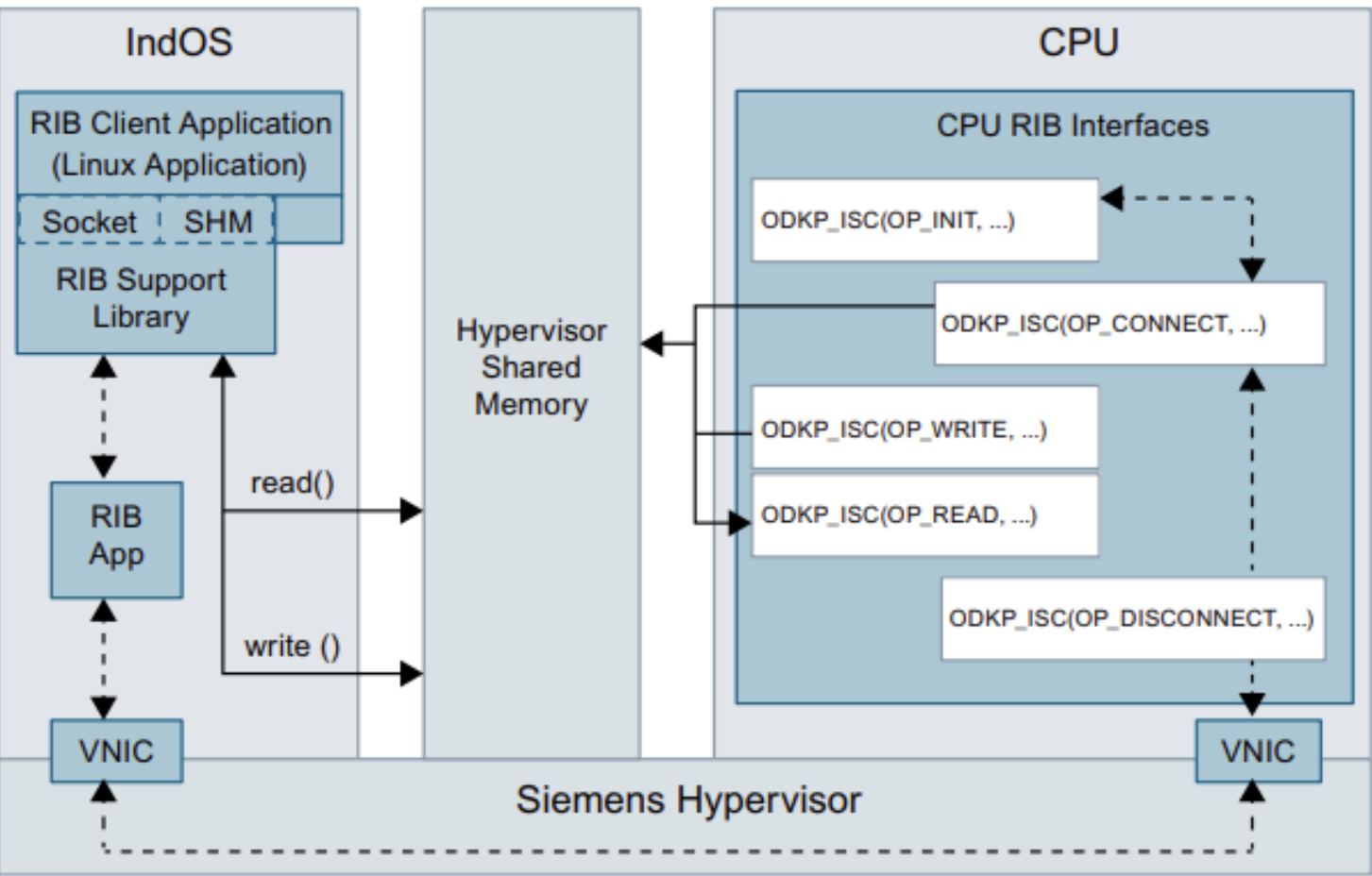


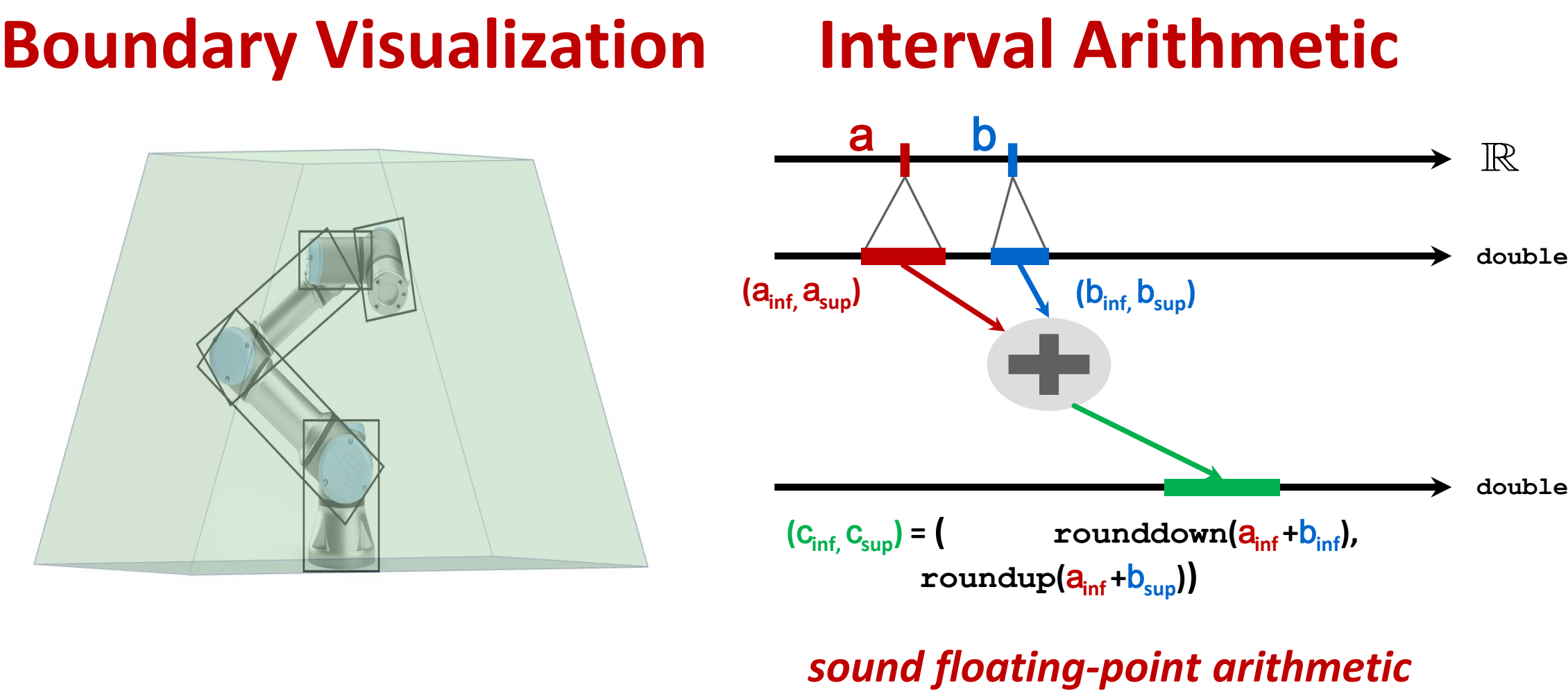
Figure 4-1 Overview of system architecture

Credit: Siemens RIB Manual

- Modern PLCs contain multiple cores, a runtime core that acts like a traditional PLC, plus a Linux core that runs a generic OS partition
- By offloading floating-point computation to the Linux core, the application space for PLCs grows
- Communication between cores is done by a shared-memory software environment called Real-time Information Backbone (RIB)

Implementation

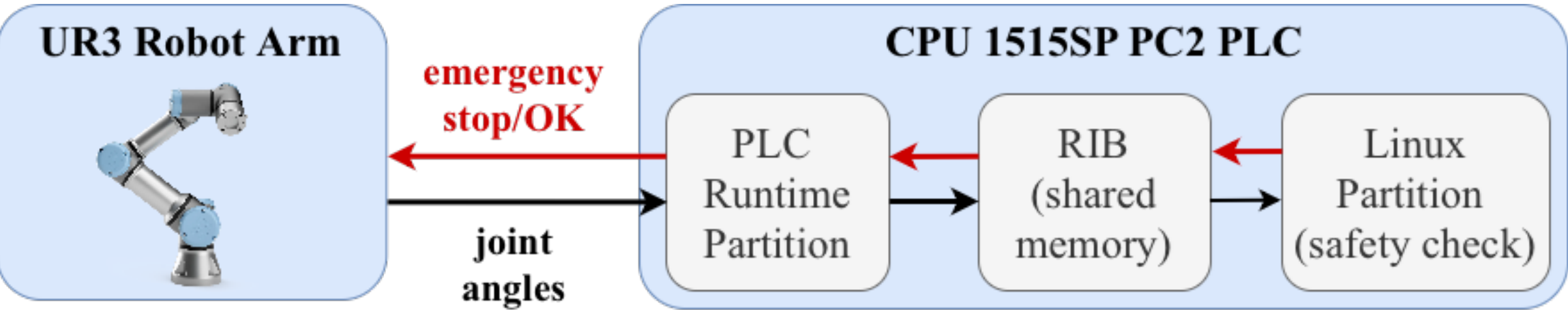
Robot Area Boundary Detection



- Model boundary around robot arm as polytope formed by a combination of planes
- Convert each joint angle into a 3D coordinate, resulting in 8 points per axis
- Utilize interval arithmetic as a method to cover floating-point imprecision and account for angular sensor error

Inter-Partition Framework

Framework Diagram



- Exchange real-time positional data via the Realtime Information Backbone (RIB) from the PLC Runtime Partition to the Linux Runtime Partition
- In the case of positional error, Linux Partition sends out an emergency stop signal through RIB to safely halt program execution before further steps are taken

Evaluation & Future Work

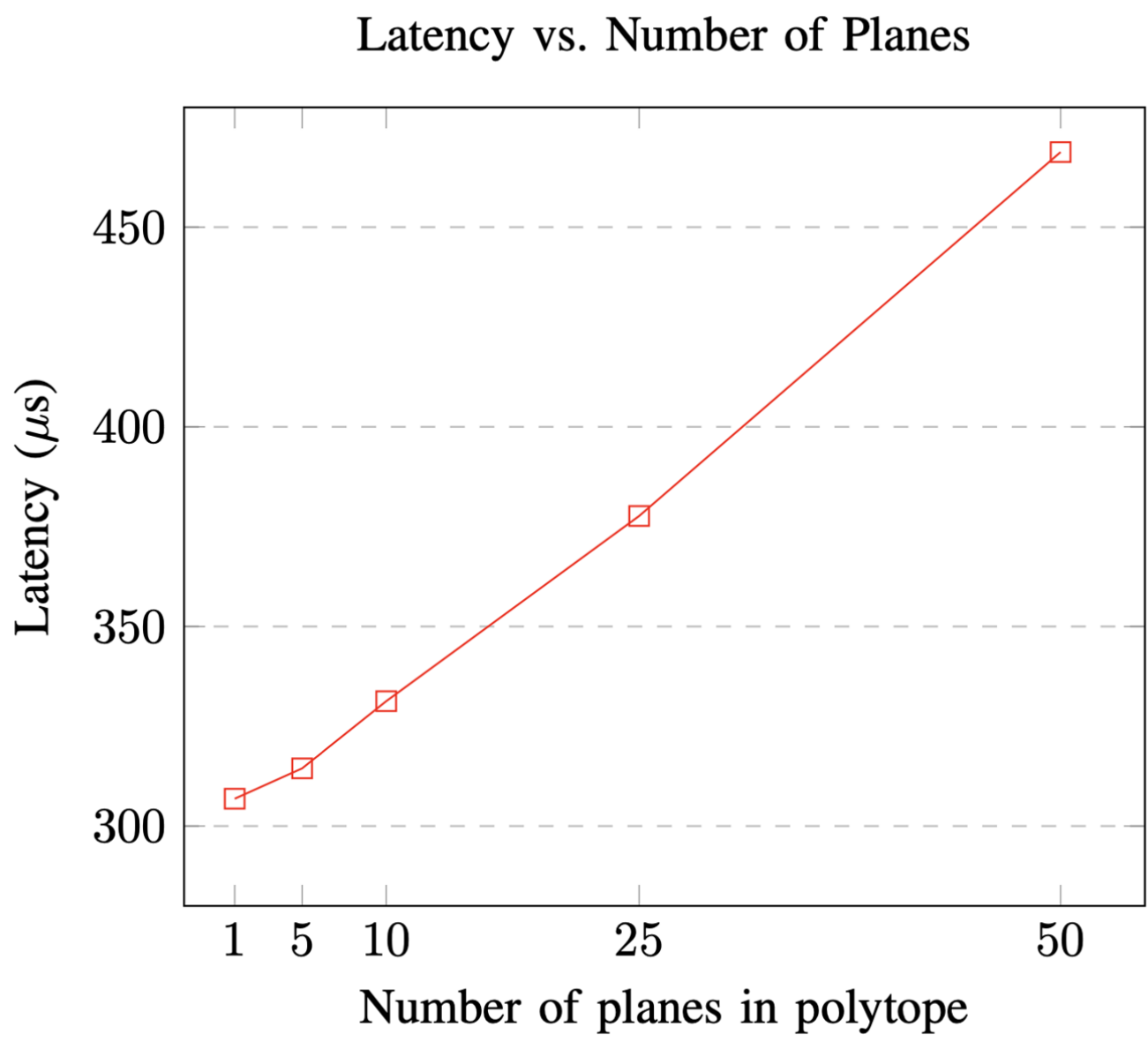
Interval Arithmetic on Linux Core

INTERVAL ARITHMETIC OPERATION LATENCY (INTEL ATOM E3940)

Category	Operation	Latency (ns/op)
Arithmetic	add	1.271
	sub	1.352
	mul	11.802
Comparison	max	1.354
	geq	2.940
Unary	abs	5.030

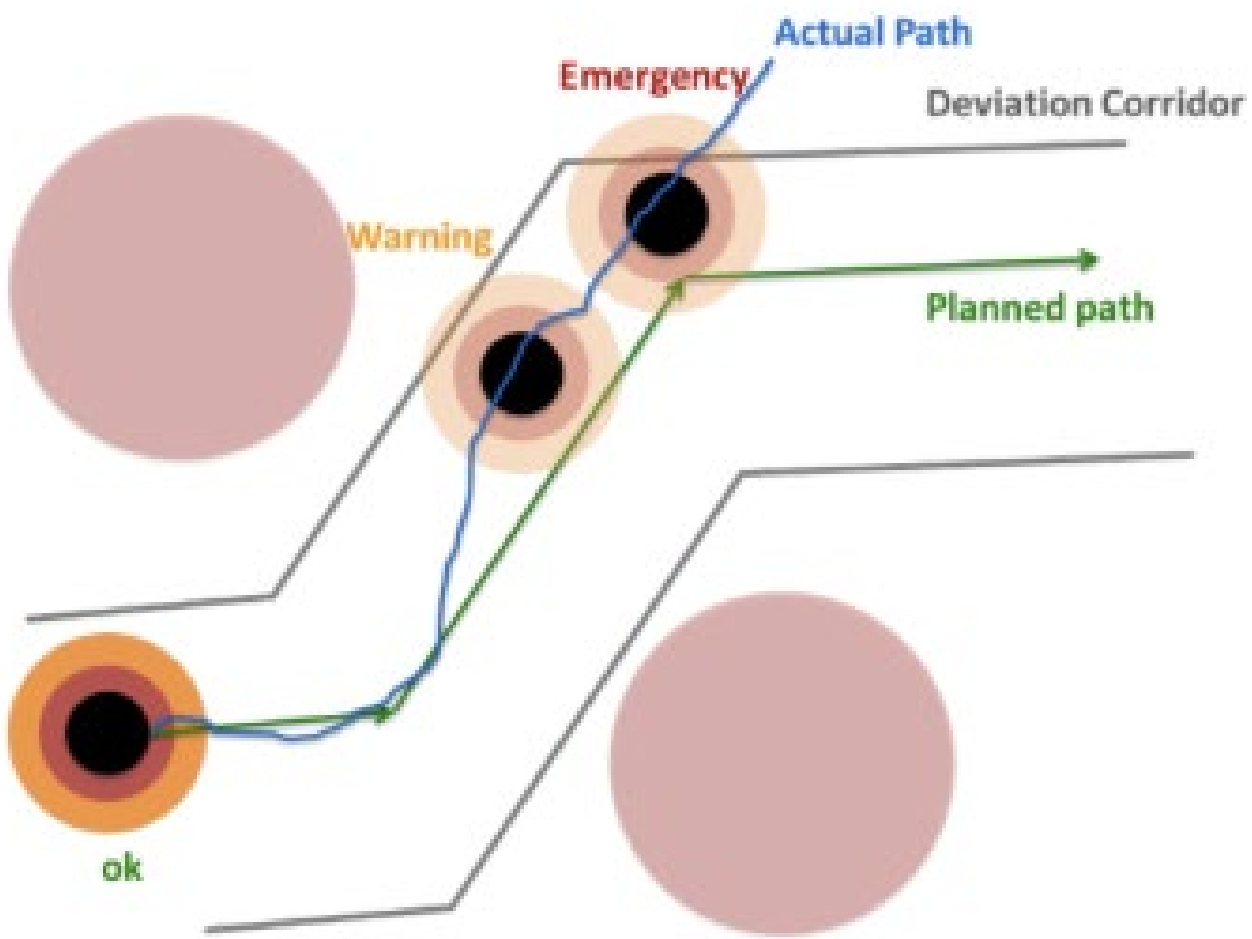
- Interval arithmetic, at its most expensive case, does not dominate program latency with overhead

Complex Geometric Boundaries on Linux Core



Future Work

- More robust path planning to improve program safety robustness
- Communication enveloping to verify data transfer across cores



Credit: High-Assurance Spiral