CPS: Medium: Secure Smart Machining

Award #1931750

Philip Levis, Dawson Engler, and David Mazières, Stanford University

This project seeks to make CNC machining safer and more secure by applying modern programming language, operating systems, networking, and cryptographic techniques to Gcode programs and their management.

Project Goals

Machining is software, but it's software from the 1960s: Gcode was standardized two years after FORTRAN

Goal: modernize CNC machining software to provide

- Integrity and auditing

- Automated checking and safety

Focus on Gcode, since all tools produce it

Historically, real-time and embedded systems have completely trusted applications: explore interactions of real-time with security and isolation.

Approaches Used

Propose a centralized architecture for optimization, integrity, and management of Gcode as well as its execution.

Use software "transforms" that operate directly on Gcode as optimizers or checkers.

Rather than rely on a cloud infrastructure, we allow CNC systems to securely and safely offload computation to local servers (e.g., for checks or optimizers) using web assembly.
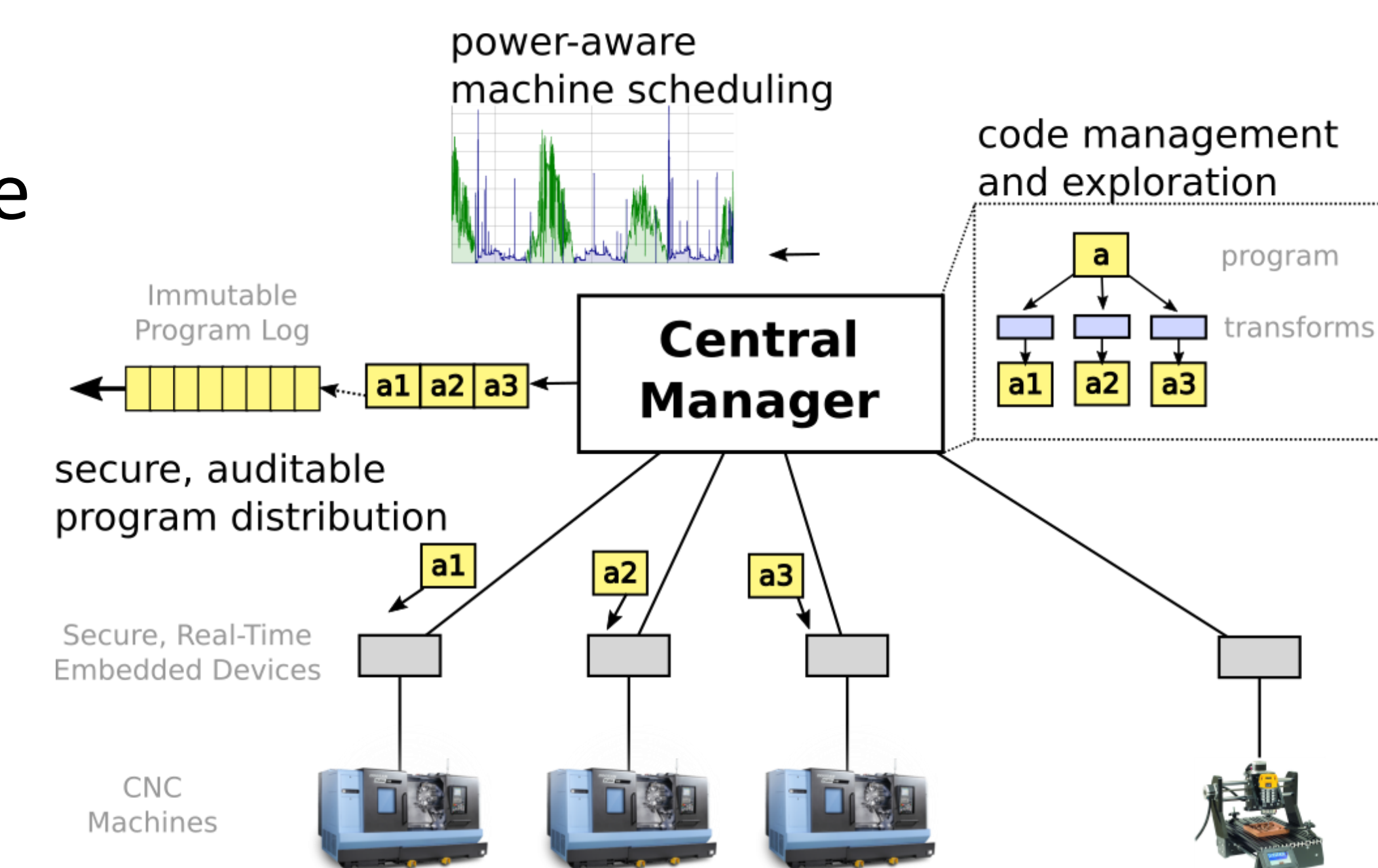
Broader Impact: Domain

Machining is fundamental to all manufacturing.

Improving the security of these systems addresses a major cyber-physical security hazard and improves efficiency.

Broader Impact: Education

As part of this grant, we have designed a new cyber-physical systems course sequence which is now an alternative systems path within the CS major.

Broader Impact : Quantify

Due to COVID-related shutdowns at the university, we have not yet been able to hold the hands-on workshops we intended, or to test our techniques on CNC systems. We are planning to do so in the next reporting period.