Rapid Certifiable Trust

Introduction

Fielding **new technologies** is essential to **preserve superiority**. However, this is only possible if these technologies are **validated for safety**.

Challenges for validation

- Growing system complexity
- Changing behavior at runtime (e.g., machine learning)
- Interactions with physical world (e.g., vehicles)
  - Correct value
  - At right time (before crash)

Methods

Formal automatic verification

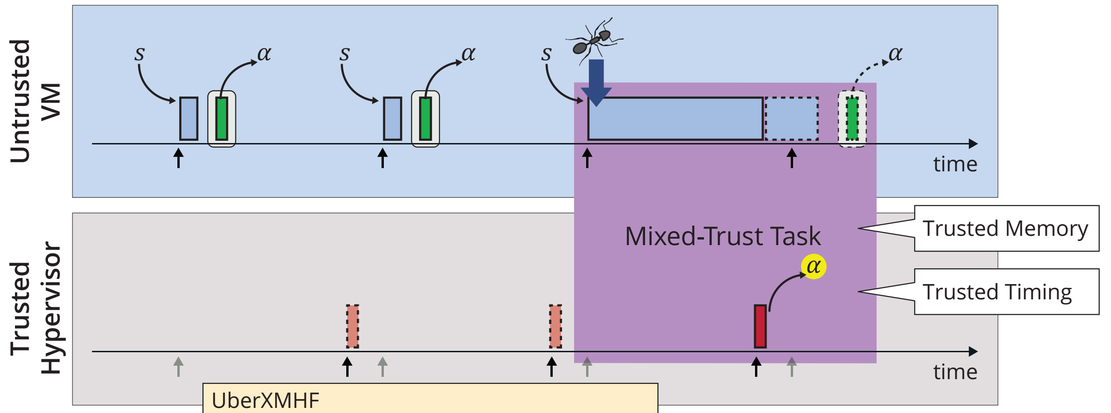
- Scalable
  - Unverified components
  - Monitored and **enforced** by verified components
  - Protected from unverified components
- Verified from
  - Physics: verify reaction of physical model (e.g., physical vehicle)
  - Logic: correct value, with correct protection
  - Timing: At the right time
- Verified protection

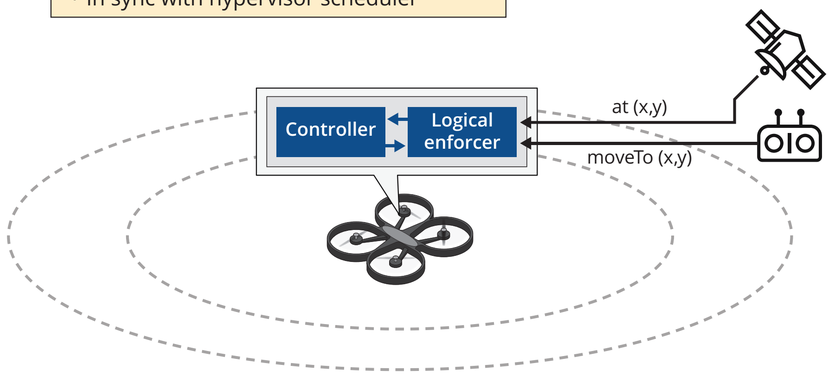
Results

- Real-Time **Mixed-Trust** Computation
- Verified protection mechanism (micro-hypervisor: UberXMHF)
- Timing verification of combined trusted/untrusted (mixed-trust)
- Physics verification of enforcement

Preserve safety by verifying only a small part of the system. **Assure trust** by protecting verified parts.

Trust = Verified + Protected





Verifying Physics

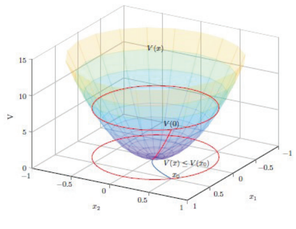
Ensure that an unverified controller cannot violate safety bounds

Controlled System: $\dot{x} = f_\varphi(x) \triangleq f(x, \varphi(x))$
Lyapunov Function: $V_\varphi : \mathbb{R}^n \to \mathbb{R}$, $\mathcal{N}_{V_\varphi}(x_{eq}) \subseteq \mathcal{N}_\varphi(x_{eq})$, $V_\phi(x_{eq}) = 0$ and $\forall x \in \mathcal{N}_{V_\varphi}(x_{eq}) - \{x_{eq}\}$: (i) $V_\varphi(x) > 0$,

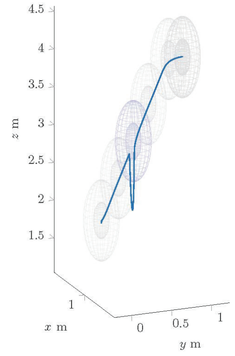
$$\dot{V}_\varphi(x) = \frac{\partial V}{\partial x} \cdot f_\varphi(x) < 0$$

Lyapunov level set:For $\epsilon > 0$,

$$\mathcal{E}_\varphi(\epsilon) = \{x \in \mathcal{N}_{V_\varphi}(x_{eq}) | V_\varphi(x) \leq \epsilon\}. \qquad \epsilon \leq 1$$

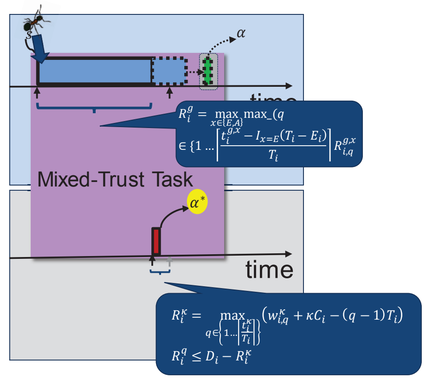


Mission: sequence of set points



Verifying Timing

Response time ≤ Deadline



Carnegie Mellon University
Software Engineering Institute

Dr. Dionisio de Niz | Dionisio@sei.cmu.edu
B. Andersson, A. Hristozov, B. Krogh, G. Moreno, A. Vasudevan

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-1044