Rapid Certifiable Trust

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

Challenges for Validation

- Increasingly complex systems
- Changing behavior at runtime (e.g., machine learning)
- Interactions with physical world (e.g., vehicles)
  - Must have correct value
  - Occur at right time (i.e., before crash)

Methods

Formal automatic verification

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

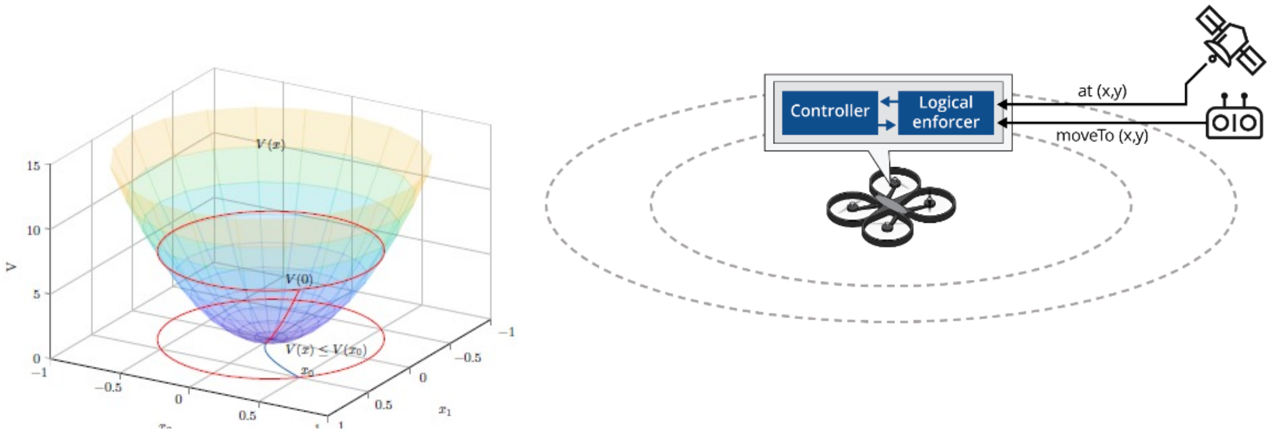
Results

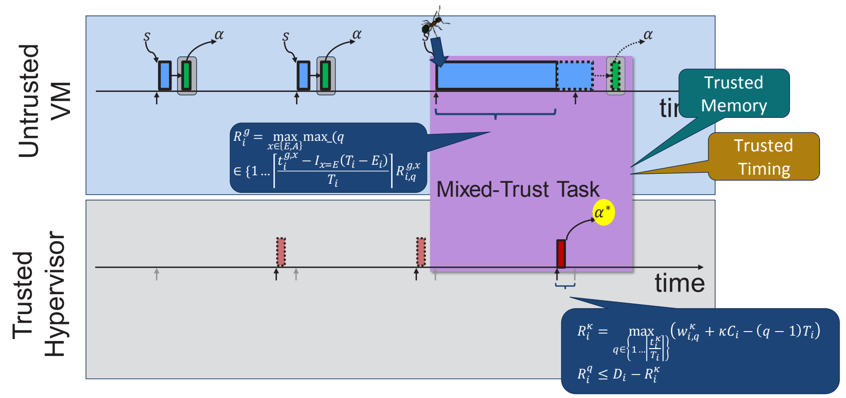
Real-time Mixed-Trust Computation

- Verified protection mechanism (micro-hypervisor: uber XMHF)
- 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 the verified part.

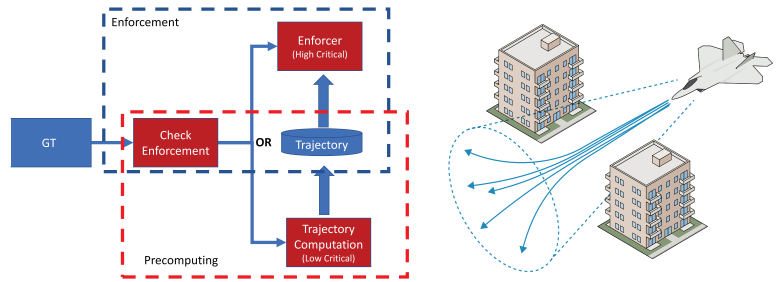
Trust = Verified + Protected





NEW RESULTS

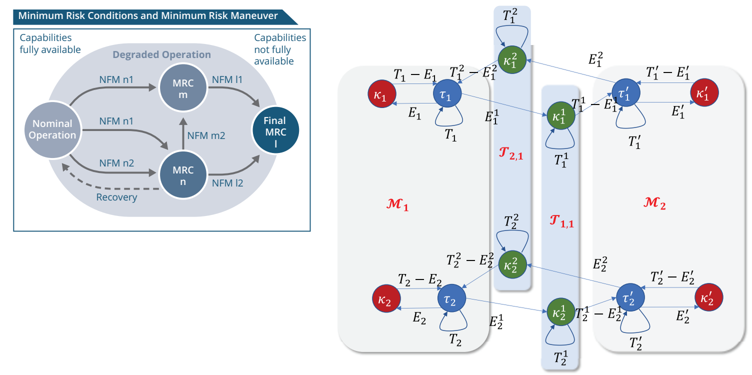
Predictive Mixed-Trust Scheduling



Balance trajectory production/consumption: $G_i^d(I_i - 1) - S_i^e \geq 0$

+ Response: $R_i^p = \kappa C_i^p + \sum \left\lceil \frac{R_i^p}{T_j} \right\rceil \kappa C_j^p - \left\lfloor \frac{R_i^p}{I_j T_j} \right\rfloor \left(\kappa C_j^p - \kappa C_j^e\right)$

Resilient Mixed-Trust Autonomy Scheduling



$$J(g_j) = \max_{v_{j,q} \in V_j} (D_{j,q} - C_{j,q})$$

$$rf_{\pi_j}^{v_{i,k}}(t) := \max\{e(\pi_j') \mid \pi_j' \text{ is prefix of } \pi_j \text{ and } end(\pi_j', v_{i,k})\}$$

$$end(\pi, v_{i,k}) = \begin{cases} p(\pi) \le t & \text{if } v_{i,k} \text{ is non-preemptive} \\ p(\pi) < t & \text{otherwise} \end{cases}$$

$$MI(v_{i,k}) = P(v_{i,k}) + \sum_{g_j \in hp(i)} rf_{\pi g_j}^{v_{i,k}}(MI(v_{i,k}) + J(g_i))$$