Scalable Assurance of CPS

Dionisio de Niz,
Principal Researcher & Technical Director
Assuring Cyber-Physical Systems

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.

DM20-1093

Scalable Assurance Challenges

Kinetic effect of Cyber-Physical Systems

- Safety critical
- Requires strong assurance
  - Logic (value)
  - Timing (before crash)
  - Correct physical reaction

Strong assurance not possible at practical scale

- Multi-Criticality:
  - But not required for everything
- Artifact size
  - Too large for strong verification techniques

Cognitive Design Overload (large systems)

- Top-level requirements -> refinement cycles -> implementation
- Assurance at all levels of refinement

Multi-Criticality

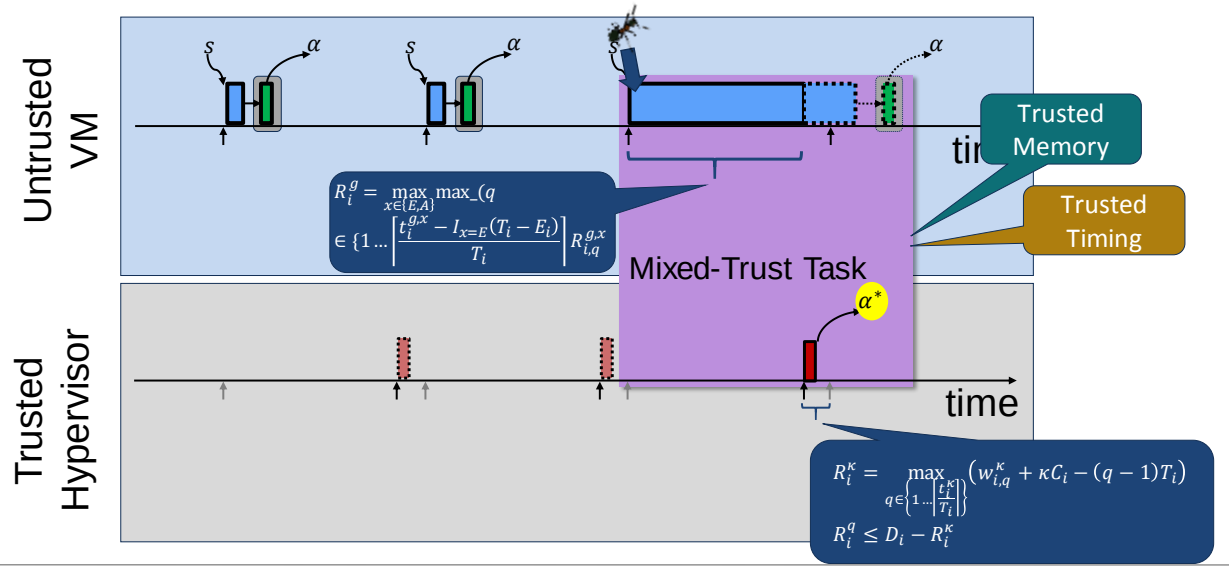
Practitioners

- DO-178 Design Assurance Levels
- Isolation between levels

Higher Criticality (Catastrophic)
Criticality (Hazardouz)
Criticality (Major)
Criticality (Minor)
Non Criticality (No Effect)

Research

- Timing: real-time mixed-criticality
  - Larger execution time -> higher assurance
  - Temporal protection
- Real-Time Mixed-Trust Computation
  - Temporal / logic protection



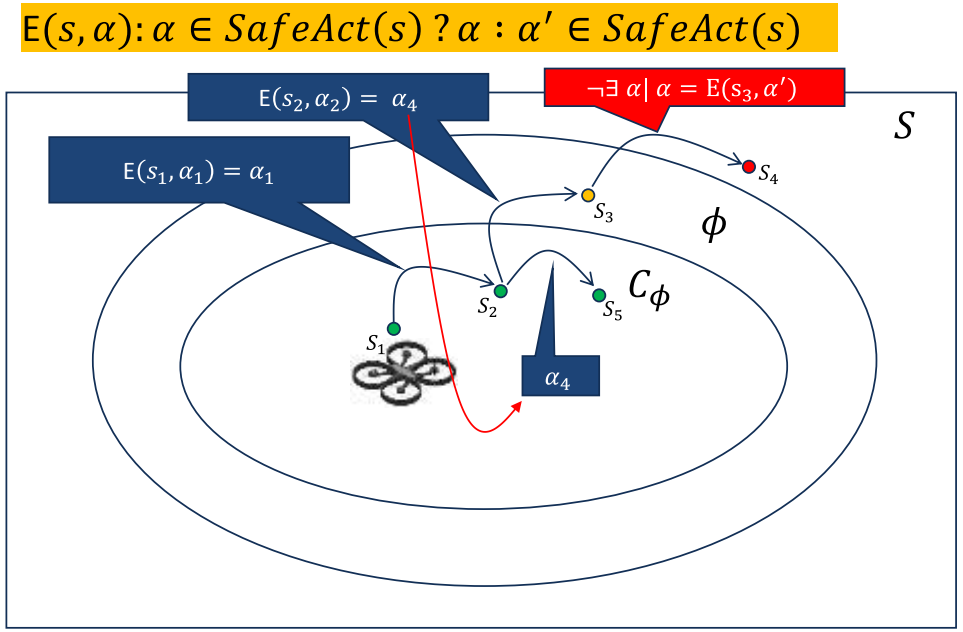
Artifact Size

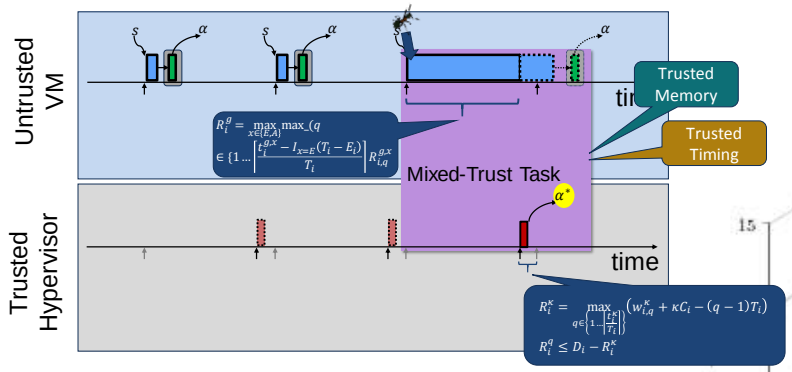
Minimize verified components
- Focus on critical properties on I/O
- Treat most system as black box

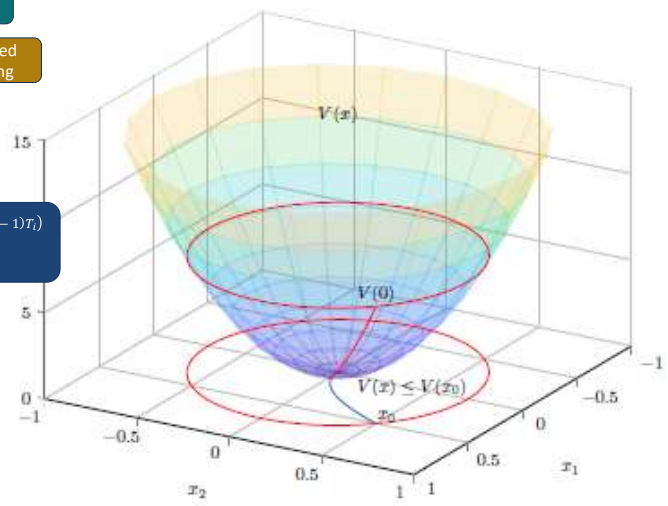
Add enforcers to guard critical property
- Small verified code to guard I/O
- Verify against critical property

Protect enforcers
- Against misbehavior of unverified components

Enforce critical aspects
- Logic
- Timing
- Physics







Cognitive Design Overload

Large CPS

- Many requirements + properties

Model-Based Engineering

- Design decisions through development (refinement)
- Continuous analyses

Analyses Assumptions

- Complex for non-experts
- Multiple domain analyses interactions