



Scalable Assurance of CPS

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



Copyright 2020 Carnegie Mellon University.

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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

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



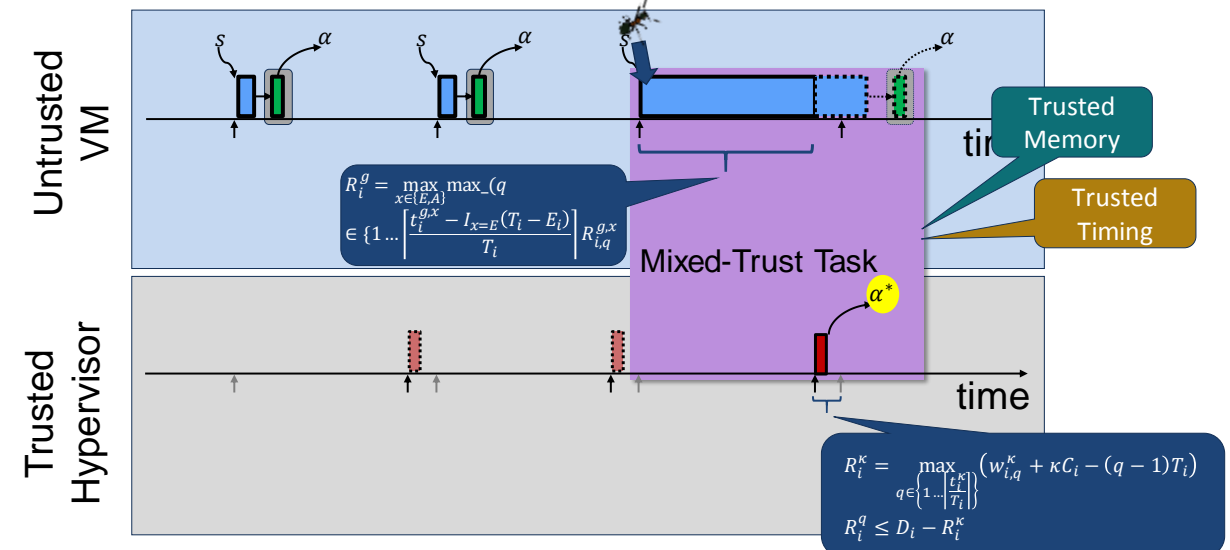
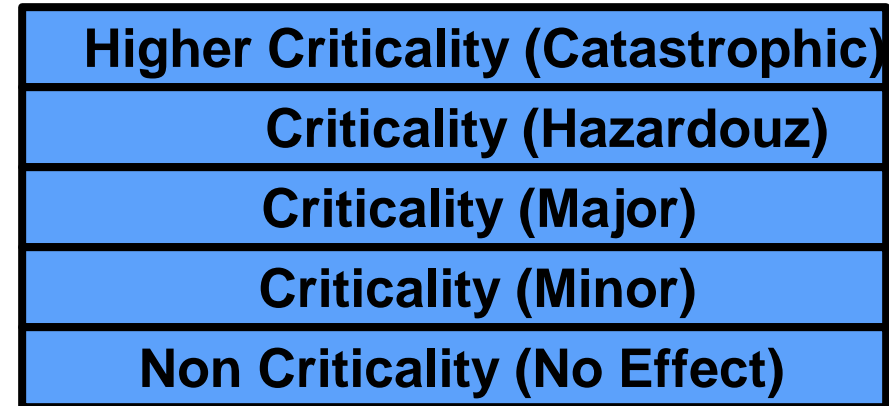
Multi-Criticality

Practitioners

- DO-178 Design Assurance Levels
- Isolation between levels

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

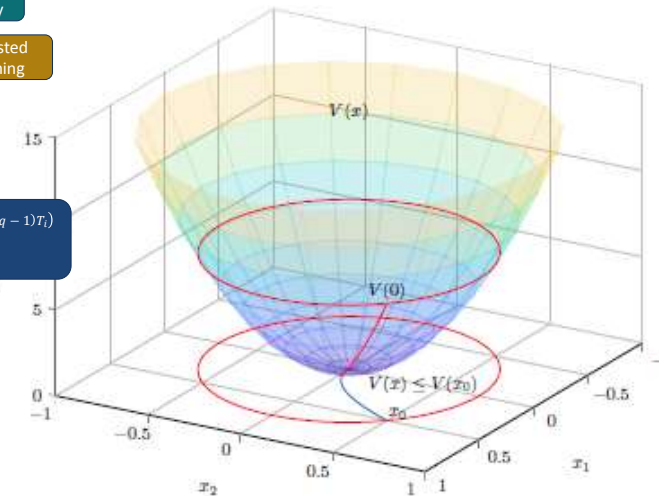
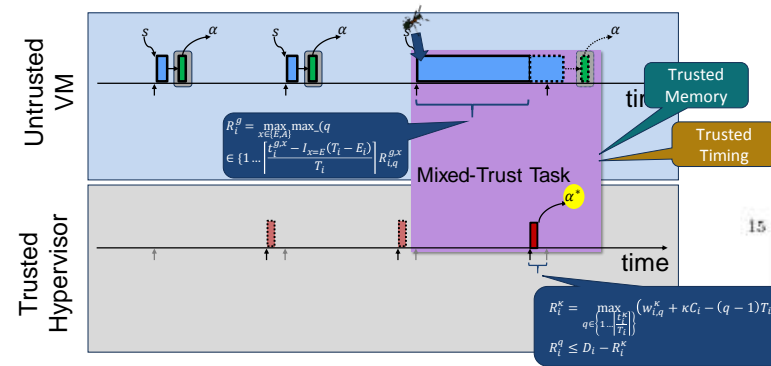
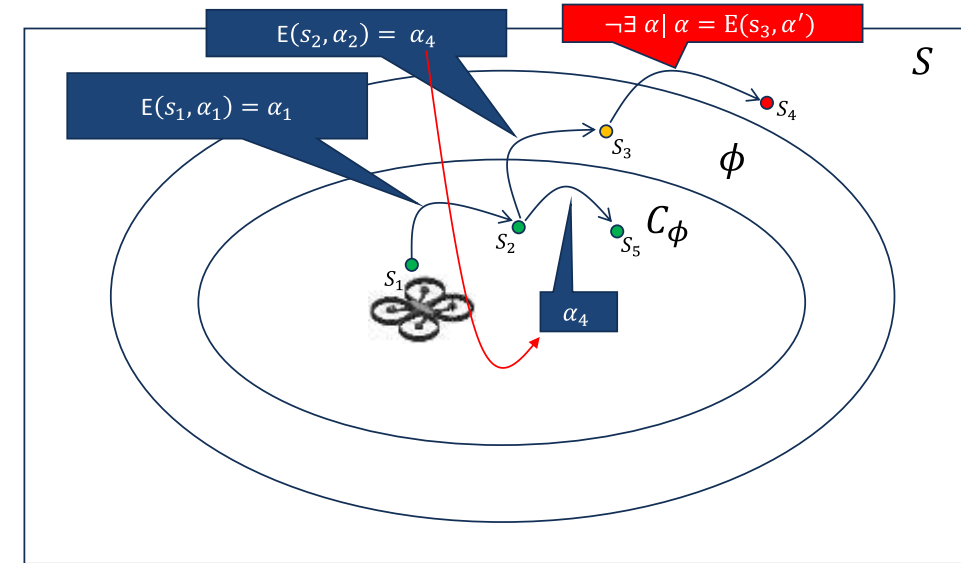
Protect enforcers

- Against misbehavior of unverified components

Enforce critical aspects

- Logic
- Timing
- Physics

$$E(s, \alpha): \alpha \in \text{SafeAct}(s) ? \alpha : \alpha' \in \text{SafeAct}(s)$$



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

