



On Design Diversity

Dionisio de Niz

Principal Researcher /
Technical Director Assuring Cyber-Physical Systems



Copyright 2022 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.

DM22-0306



Design Diversity

Design diversity targets misbehavior that cannot be detected/corrected without variants

Two Main Challenges

Misbehavior detections

Misbehavior correction



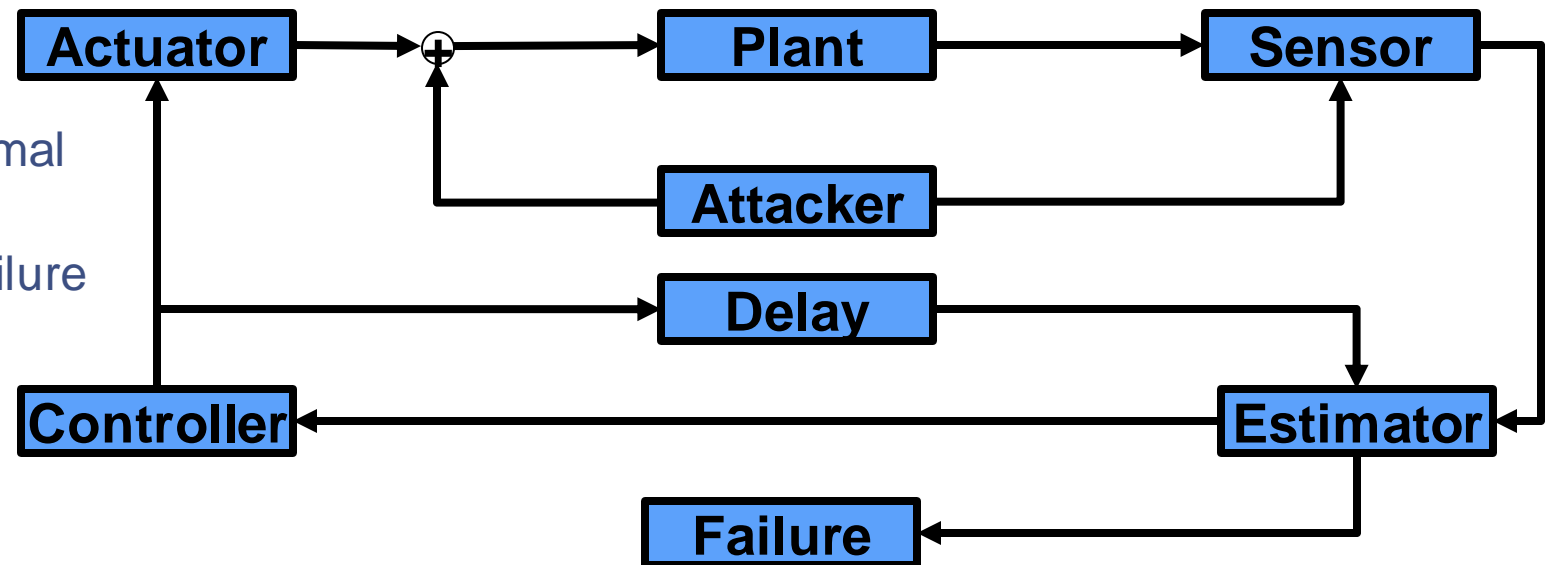
On Misbehavior Detection (1)

In a CPS it is possible to detect misbehavior without diverse sensors

From Security Literature (misbehavior can be error or attack)

Physical Water Marking¹

- Embed random signal in control
- Estimate response from plant not anticipated by attack or signals normal behavior
- If anticipated signal not present: Failure



¹Cyber-Physical Systems, R. Rajkumar, D. de Niz, M. Klein, Addison Wesley, 2017

On Misbehavior Detection (2)

Attacker/ Error Can Prevent Detection

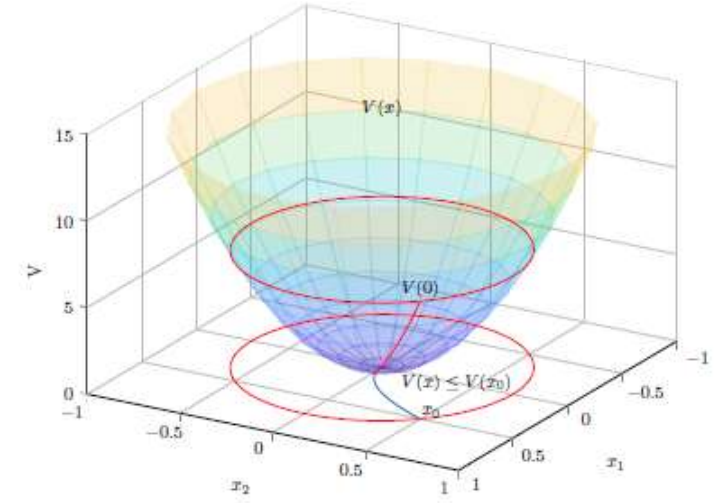
But we can

- Ensure Worst Damage is Tolerable
- Recoverable Set: $\varepsilon_{SCj}(1)$ Safety Set: $\varepsilon_{SCj}(\varepsilon_s) \triangleq \varepsilon_s \varepsilon_{SCj}(1)$
 - Controlled System: $\dot{x} = f_\varphi(x) \triangleq f(x, \varphi(x))$
 - Lyapunov Function:

$$V_\varphi: \mathbb{R}^n \rightarrow \mathbb{R}, \mathcal{N}_{V_\varphi}(x_{eq}) \subseteq \mathcal{N}_\varphi(x_{eq}), V_\varphi(x_{eq}) = 0, \forall x \in \mathcal{N}_{V_\varphi}(x_{eq}) - \{x_{eq}\}: (i) V_\varphi(x) > 0,$$
$$\dot{V}_\varphi(x) = \frac{\partial V}{\partial x} \cdot f_\varphi(x) < 0, \text{ level set: } \varepsilon_\varphi(\varepsilon) = \{x \in \mathcal{N}_{V_\varphi}(x_{eq}) \mid V_\varphi(x) \leq \varepsilon\}, \varepsilon \leq 1$$

Until we can recover to a known state

- Periodic Fast Reboot:
 - Checkpoint
 - Rollback



Misbehavior Correction

Without Detection

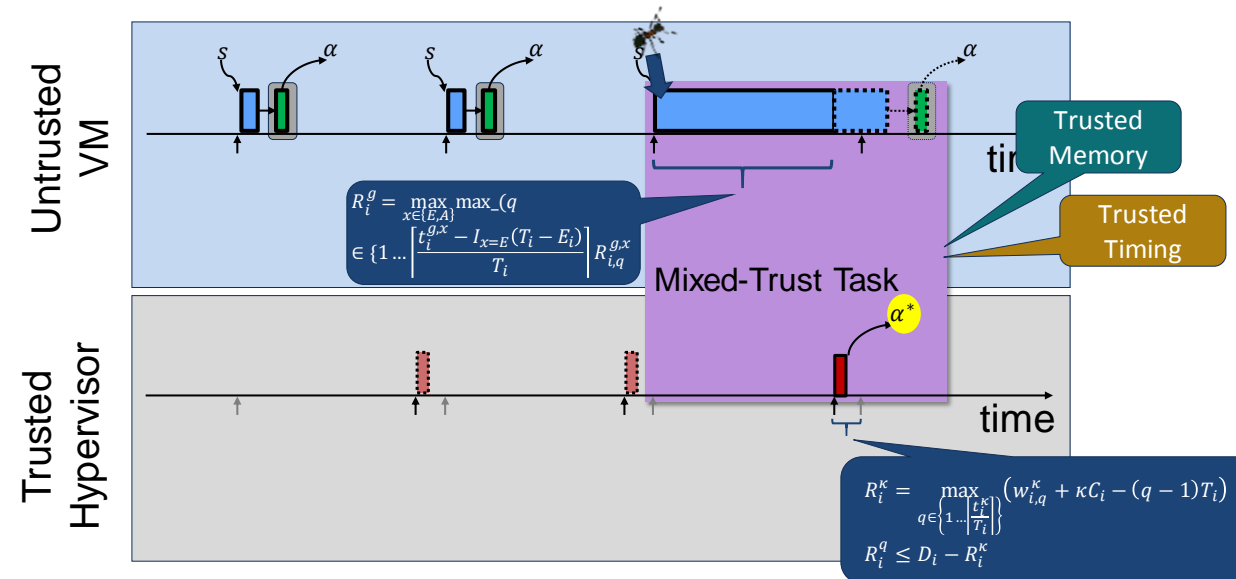
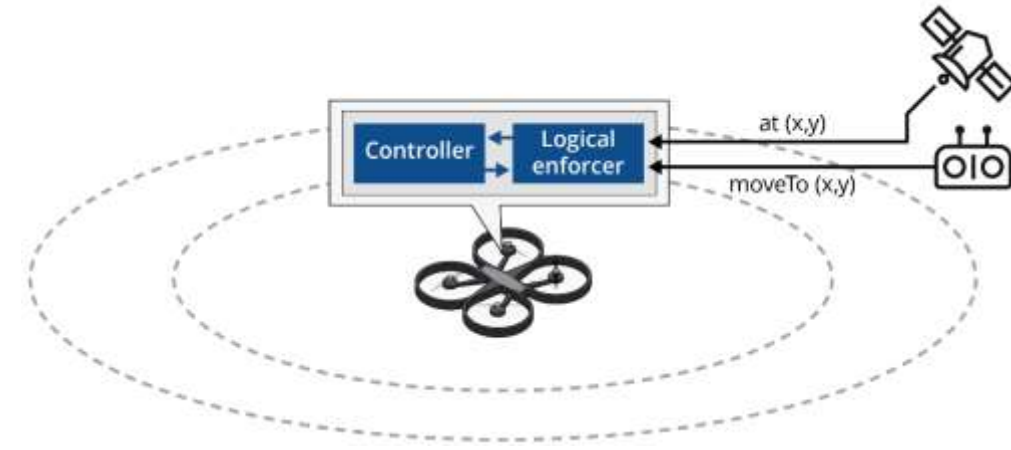
- Periodic Reboot
 - Frequent enough to prevent damaging errors/attacks
 - But allow mission to progress / prevent instability
- Protect image “clean” image (checkpoint)

With detection

- Monitor behavior (safe output)
 - Replace with safe output (enforcement)

Protection

- Timing faults
 - Real-Time Mixed-Trust¹
- Memory Faults
 - Verified Hypervisor²



¹D. de Niz, B. Andersson, M. Klein, J. Lehoczy, A. Vasudevan, H. Kim, & G. Moreno. Mixed-Trust Computing for Real-Time Systems. IEEE RTCSA, 2019.

²A. Vasudevan, P. Maniatis, R. Martins, S. Chaki. Practical, Provable, End-to-End Guarantees at the Edge. USENIX Workshop on Hot Topics in Edge Computing 2020



Concluding Remarks

Design Diversity May Not Be Necessary

- If we can detect and contain misbehavior
- Or anticipate worst damage and contain it

Lessons from Security Domain

- Deviations from normal behavior can be detected through models
- Multiple type of properties must be consider in Cyber-Physical Systems
 - Value correctness
 - Timing correctness
 - Physical effect correctness

Protection need to isolate critical components from failures

