Consensual Resilient Control

Aleksandar Matovic, Rafal Graczyk, Federico Lucchetti, Marcus Völp
University of Luxembourg, SnT, CritiX group
firstname.lastname@uni.lu

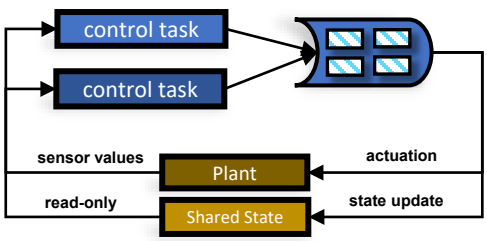
CRITIX

Real-Time Control with just a detection quorum

- Resilient consensual control with **f+1** instead of **2f+1** replicas
- Leveraging the inherent plant stability to tolerate several deadline misses allows us to operate with just detection quorum

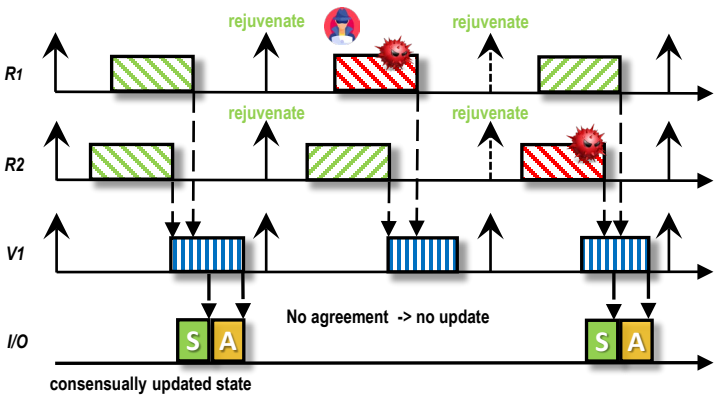
Replicated control architecture

- Control task replicas monitor the plant, suggest actuation signals and state updates, which are adopted after voter consensus



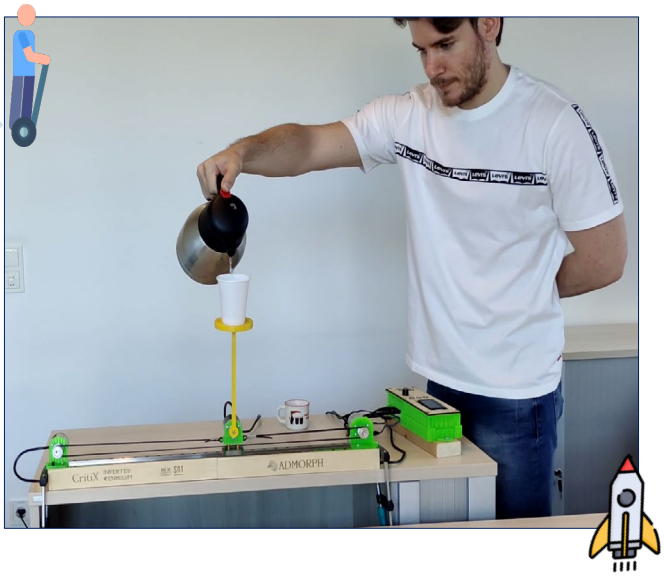
Detect, adapt and mask

- In the first invocation, correct replicas agree. In the second, the agreement fails due to Replica 1's failure. In the third epoch, the voter collects enough (f+1) similar proposals after the revival of both R1 and R2, despite Replica 2's failure.



Don't let the hackers spill your coffee

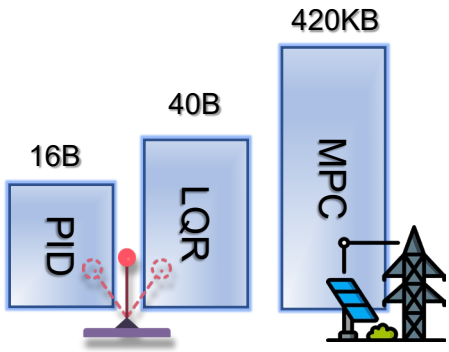
stay in control despite the difficulties



- The stabilization problem is often exemplified by an inverted pendulum, which is commonly featured in textbooks. The same algorithm used for its stabilization can also be found in Segways and rocket stabilization thrusters.

Controller's shared state

- The share state of the controller depends on the specific control algorithm. While it's only a few variables for an inverted pendulum, it can reach up to 420KB per invocation step in an electric microgrid scenario



In collaboration with:
ADMORPH and the industry partners: SYSGO EMBEDDING INNOVATIONS, Q-media, THALES, Collins Aerospace

More about CritiX here: