Integrated Reconfigurable Control and Moving Target Defense for Secure Cyber-Physical Systems

Bradley Potteiger (Johns Hopkins APL), Zhenkai Zhang (Texas Tech), and Xenofon Koutsoukos (Vanderbilt)
https://cps-vo.org/group/mtd

Motivation

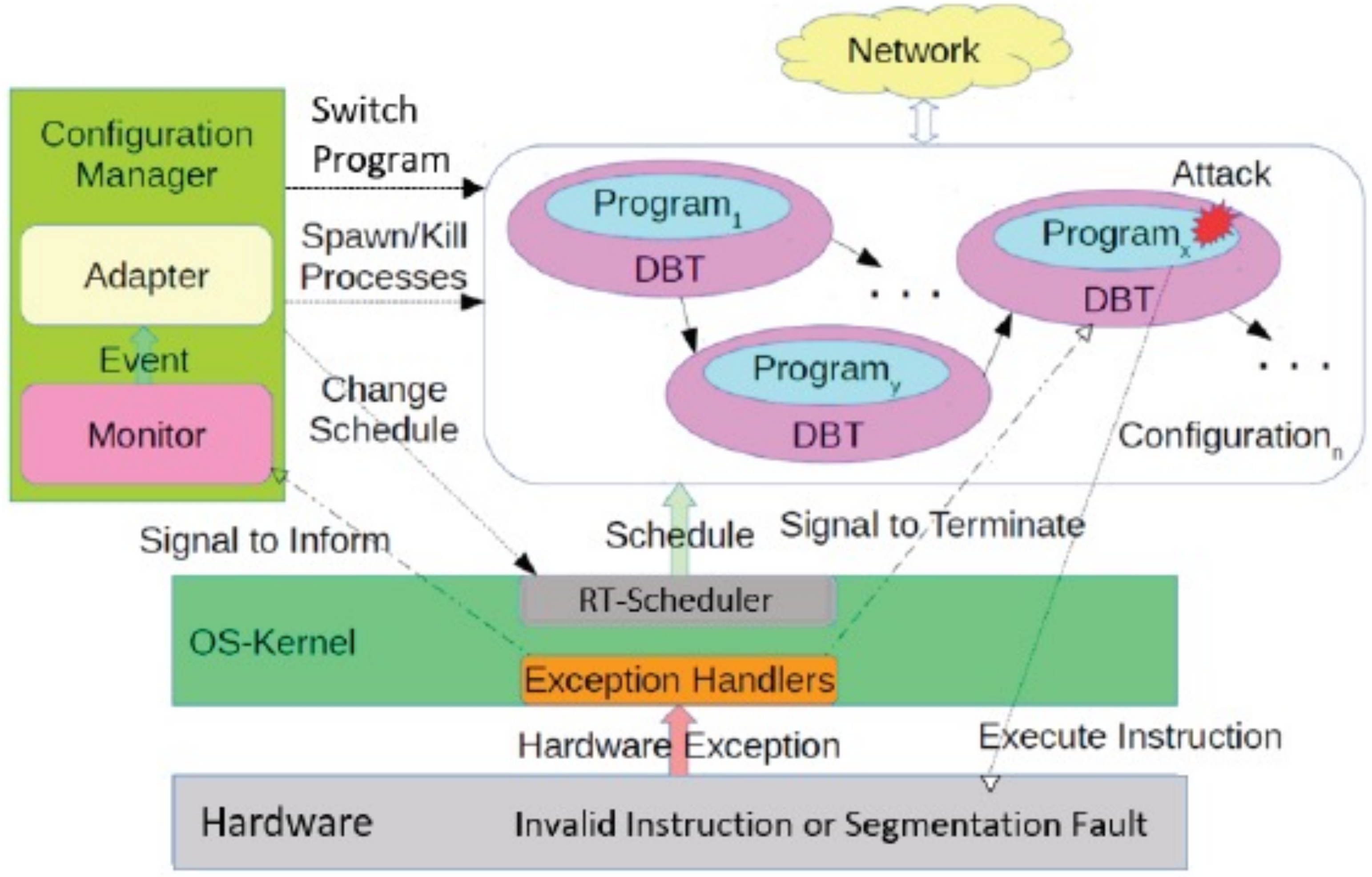
- CPS-IoT are increasingly subjected to sophisticated cyber-attacks
- Tightly coupled nature between the CPS software and physical dynamics
- Memory corruption attacks exploit can compromise CPS safety
- CPS not only have to maintain integrity while under cyber attacks, but also need to ensure safe operation

Challenge

- Integrated reconfigurable control and moving target defense for securing CPS

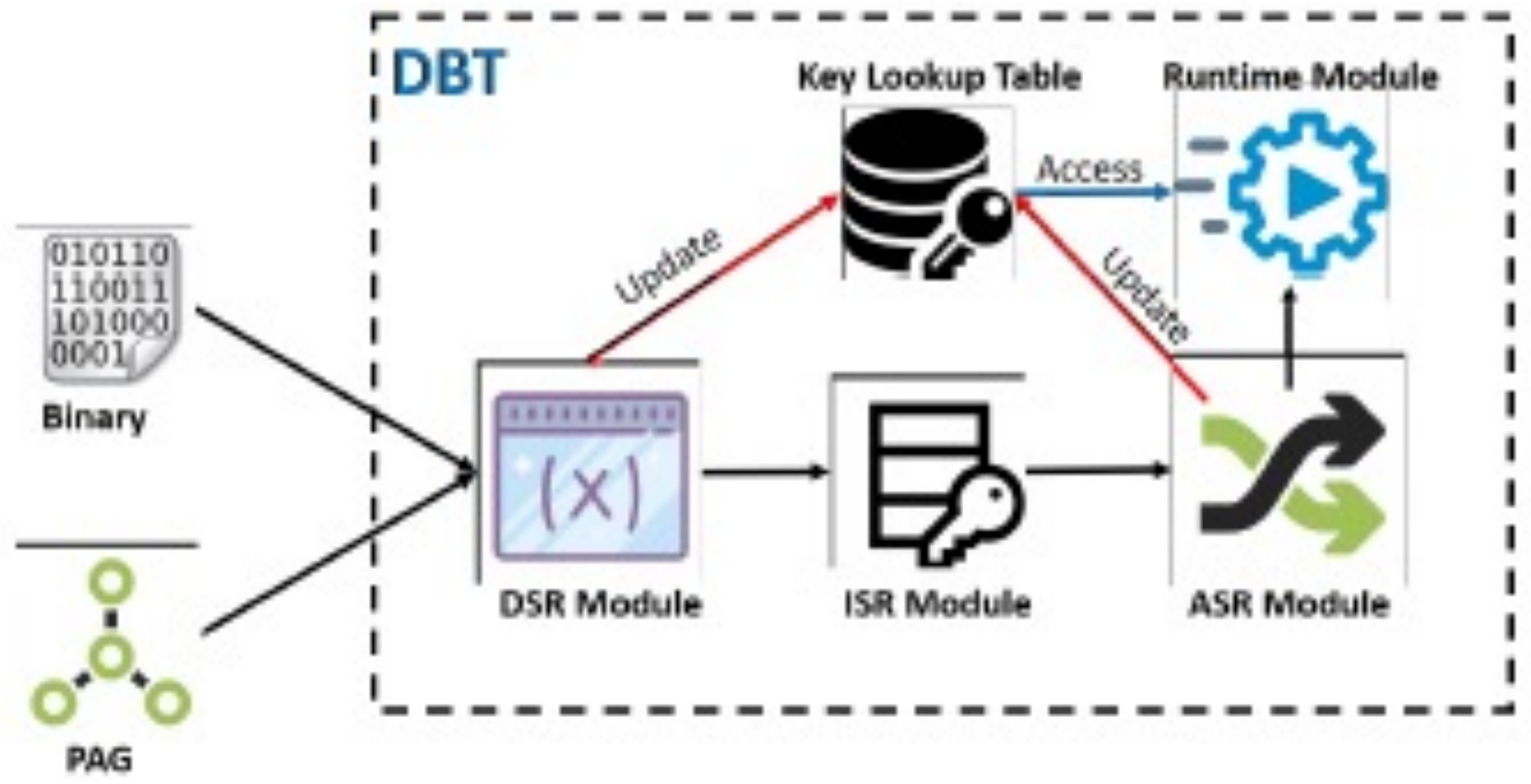
Solution

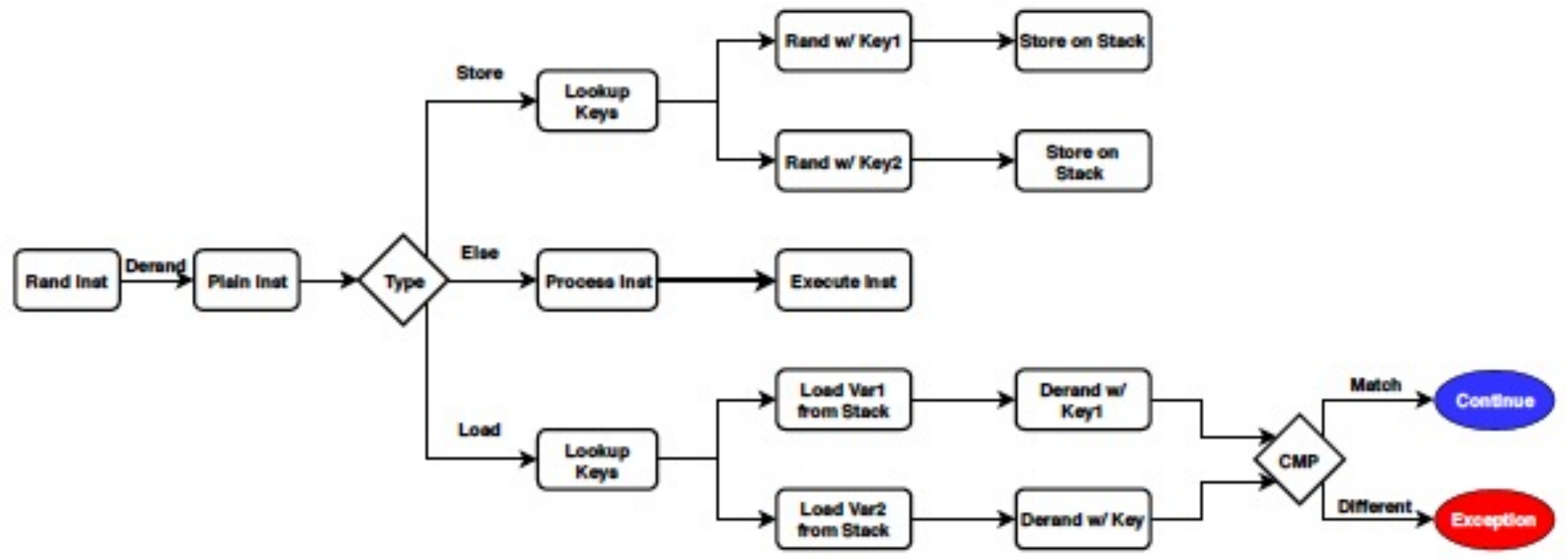
- Security in Mixed Time and Event Triggered CPS using Moving Target Defense



Security Architecture

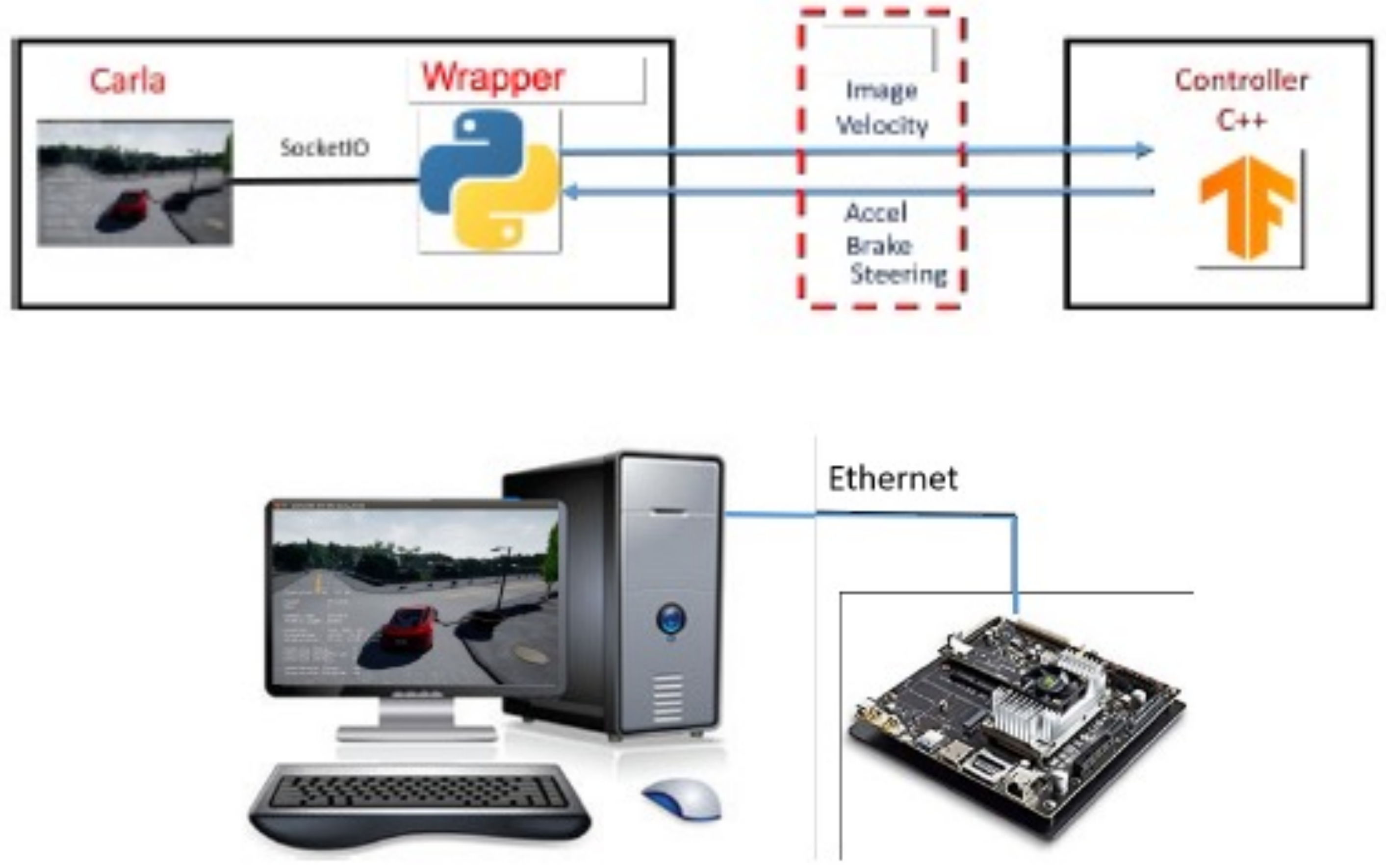
MTD Initialization Process

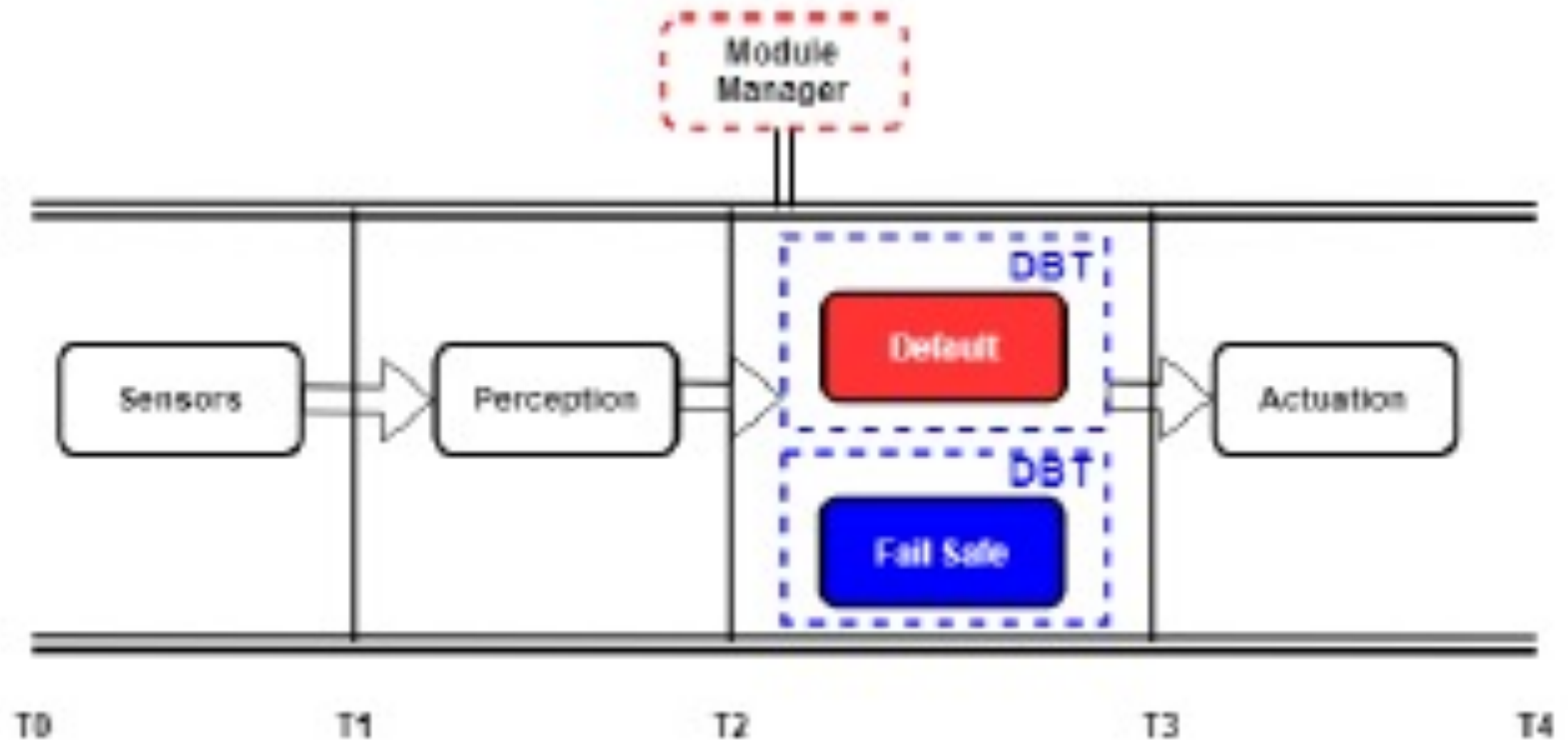




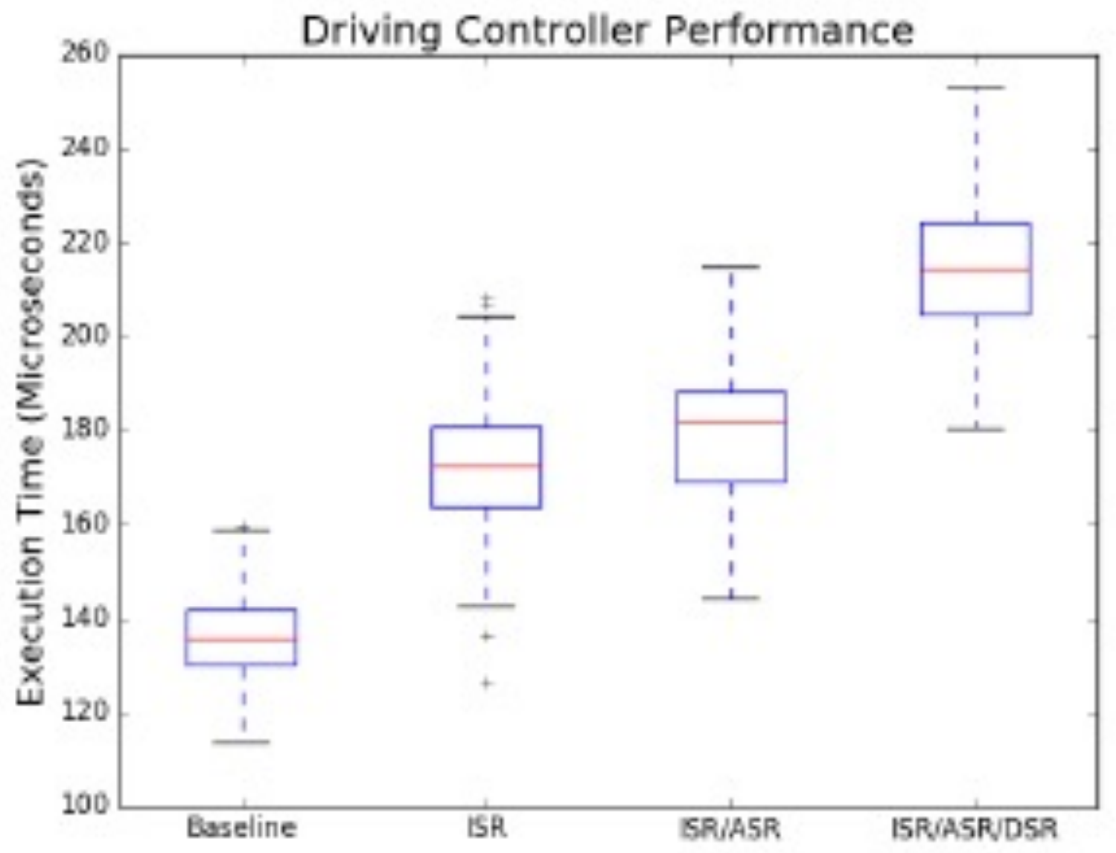
MTD Runitime Process

Hardware-in-the-loop Testbed

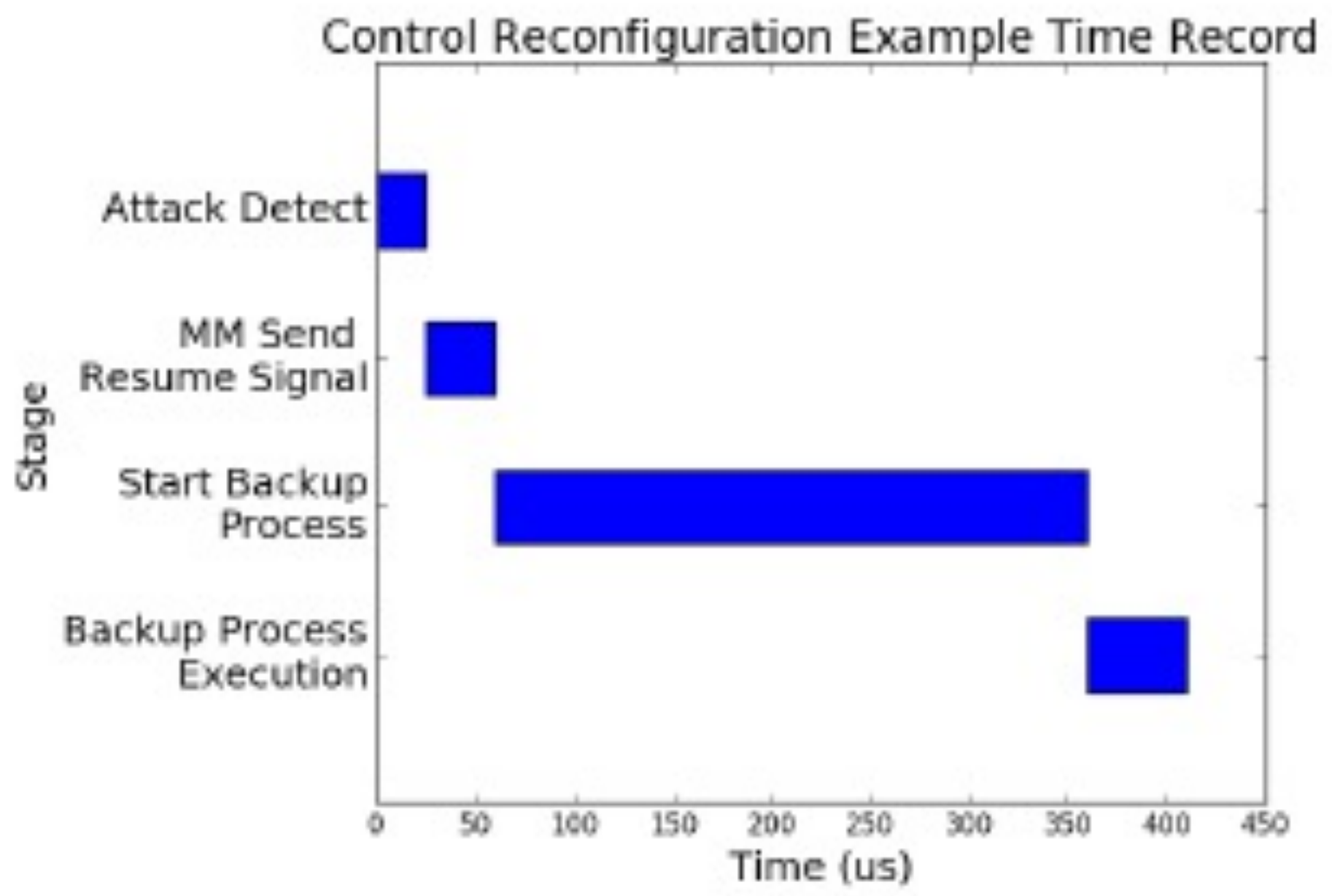




Schedule and Reconfiguration



Execution Times



Control Reconfiguration Example

Broader Impact

- The project contributions can be used to protect safety-critical CPS against cyber attacks
- Undergraduate research
- Transition activities
  - NSF I-Corps
  - Won Southeast Entrepreneurship Conference's Student Pitch Competition

2021 NSF Cyber-Physical Systems Principal Investigators' Meeting
June 2-4, 2021

Award ID#: CNS-1739328