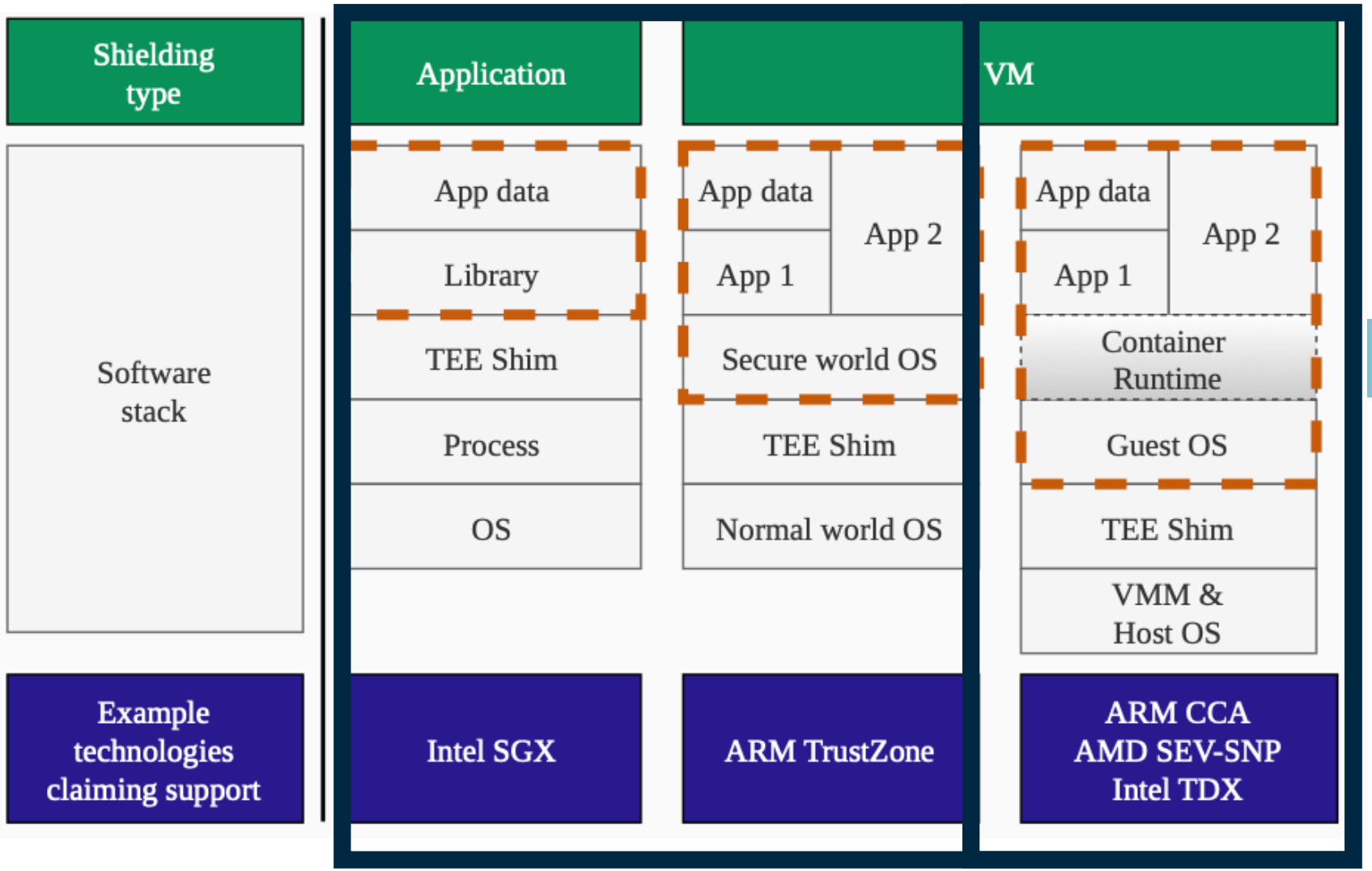
UNIVERSITÄT ZU LÜBECK

SEV-Step

A Single-Stepping Framework for AMD-SEV

Luca Wilke, Jan Wichelmann, Anja Rabich and Thomas Eisenbarth



Single Stepping

Single-Stepping Attacks

Idea, Exploits, Root Cause

UNIVERSITÄT ZU LÜBECK

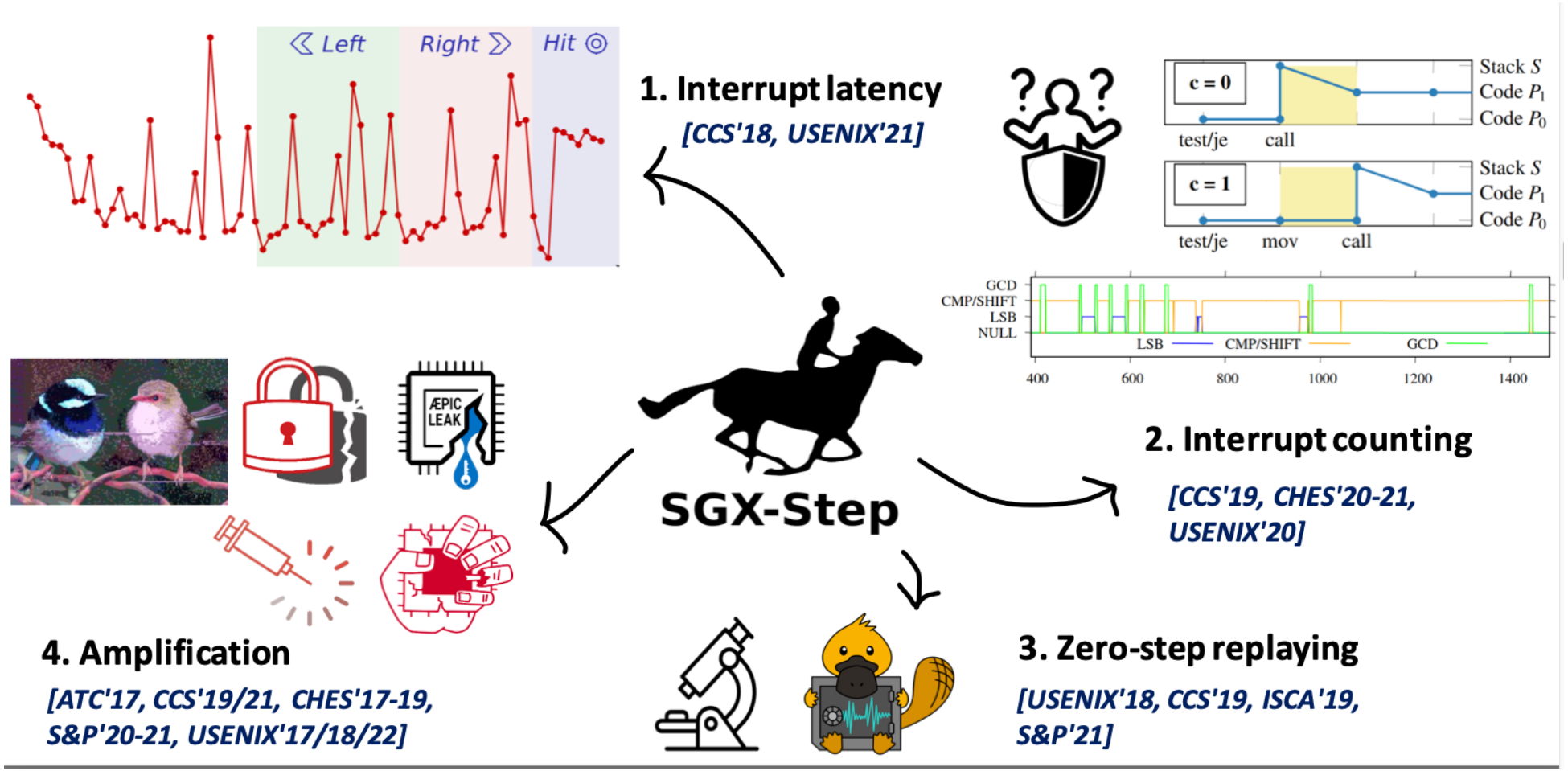
Single-Stepping: Idea

normal

frequently interrupted

single-stepped

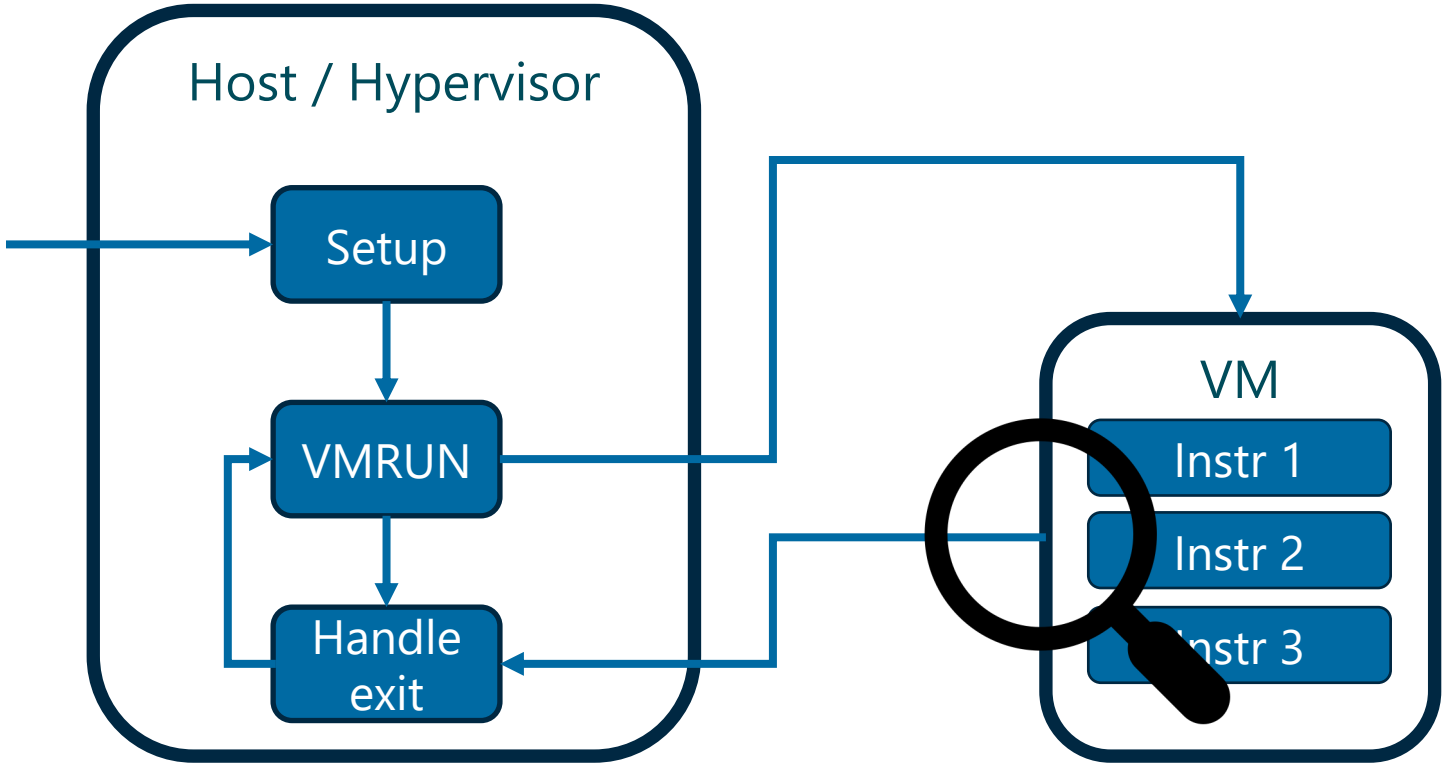
Single-Stepping: Attack Avenues



SGX-Step

Can SEV VMs be single-stepped?

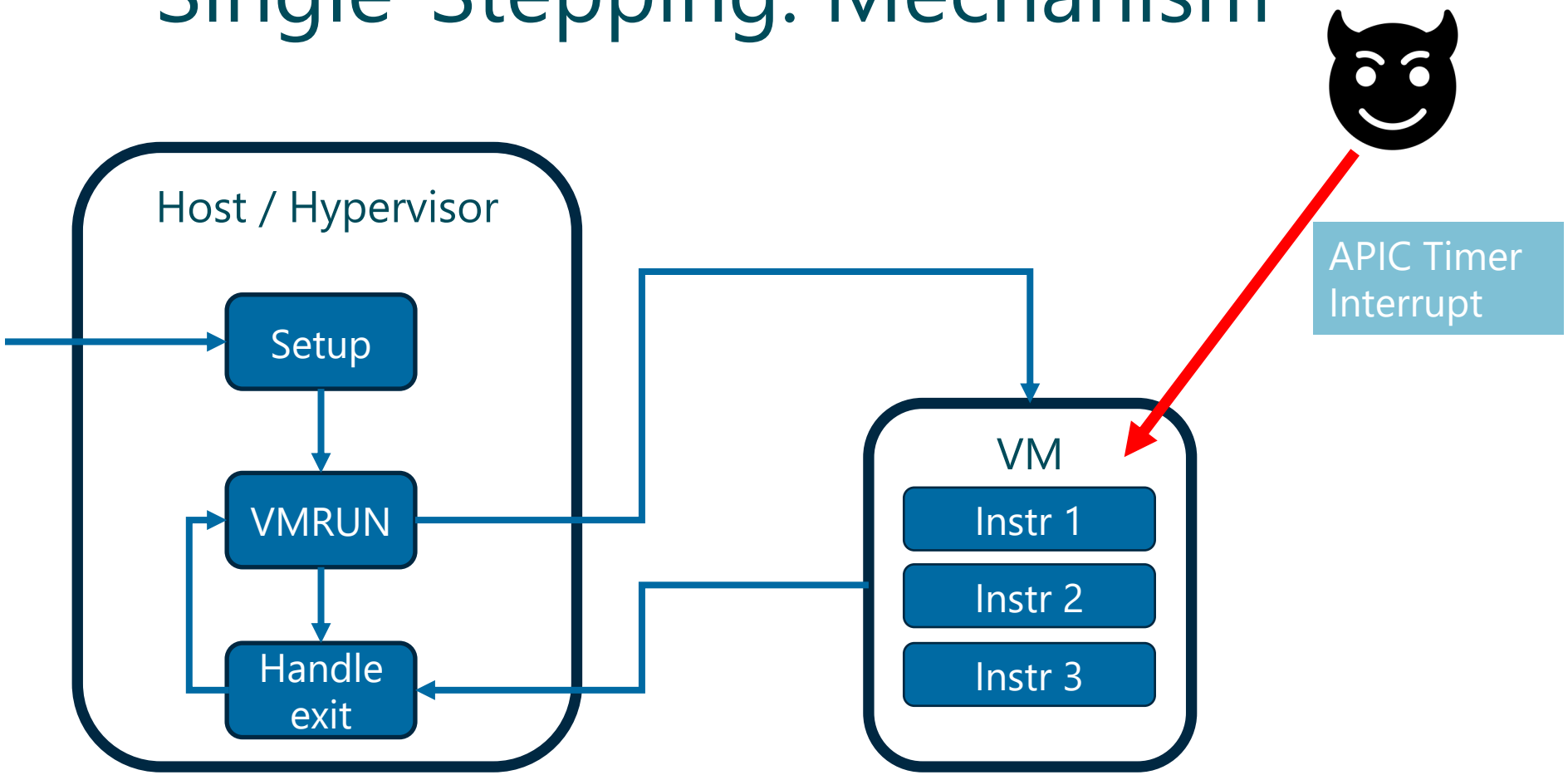
Single-Stepping: Mechanism



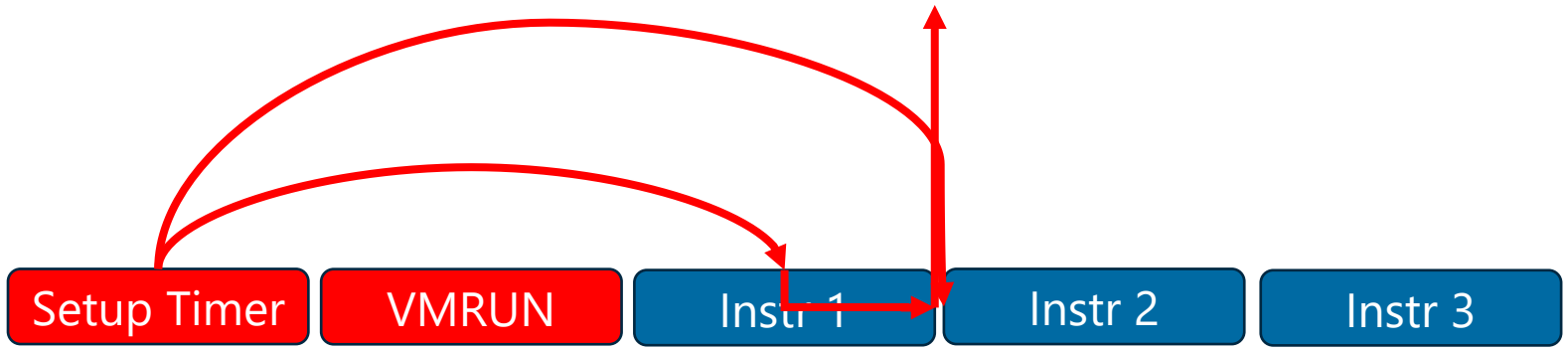
When do we exit?

- Intercepted Instruction
- Page Fault
- External Interrupt

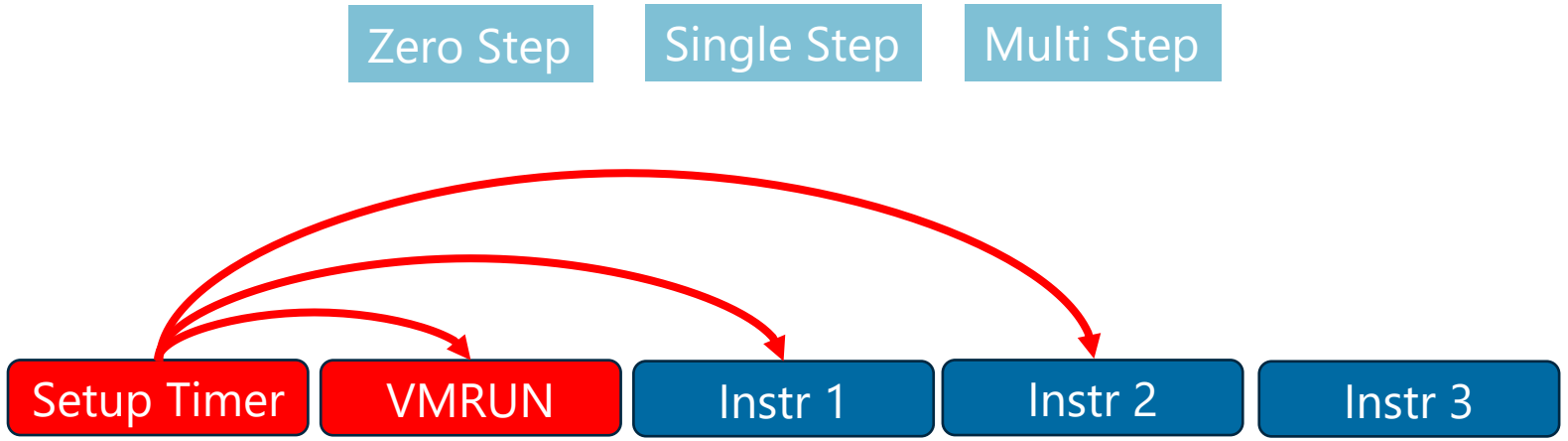
Single-Stepping: Mechanism



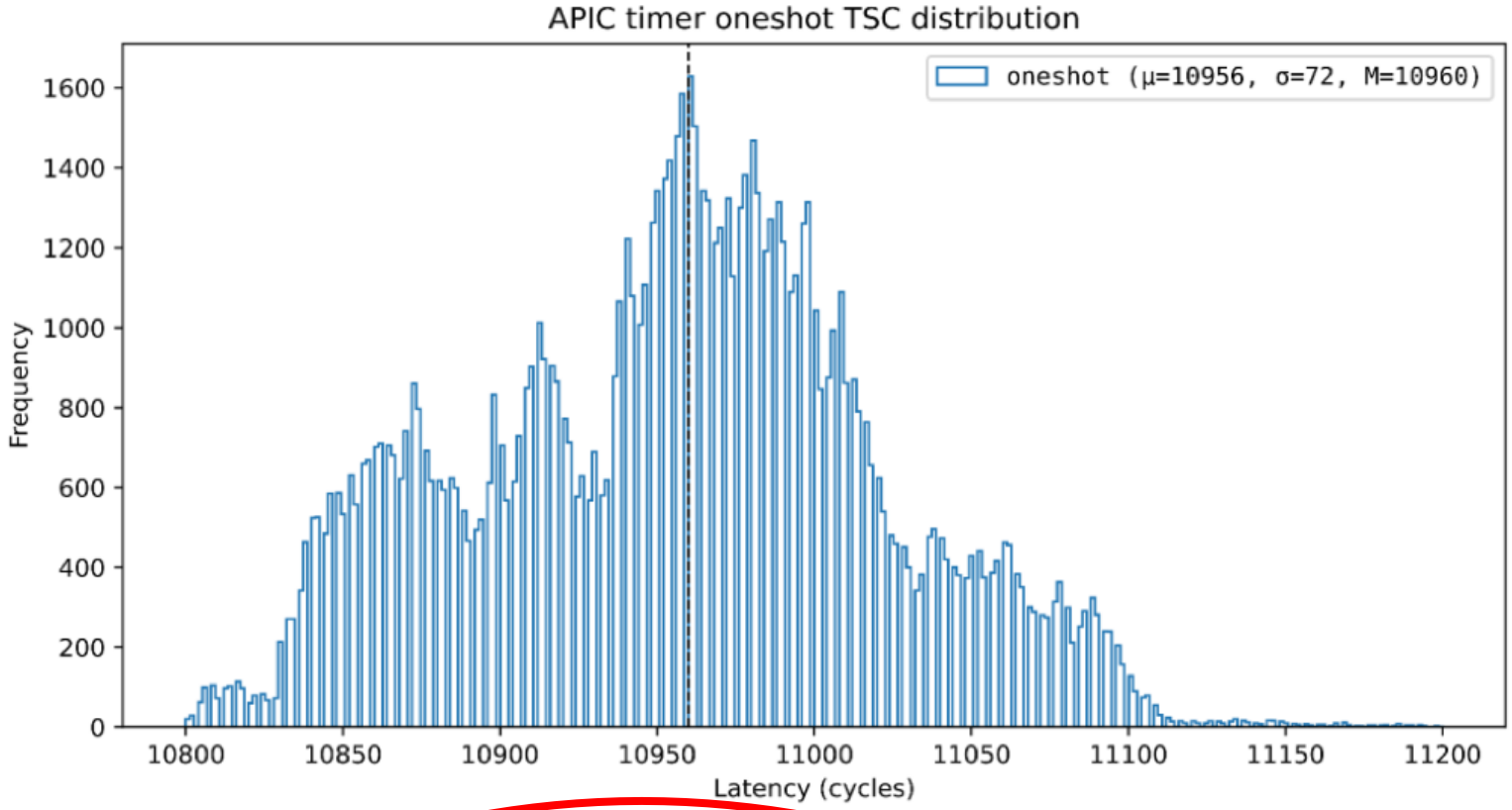
Single-Stepping: Root Cause



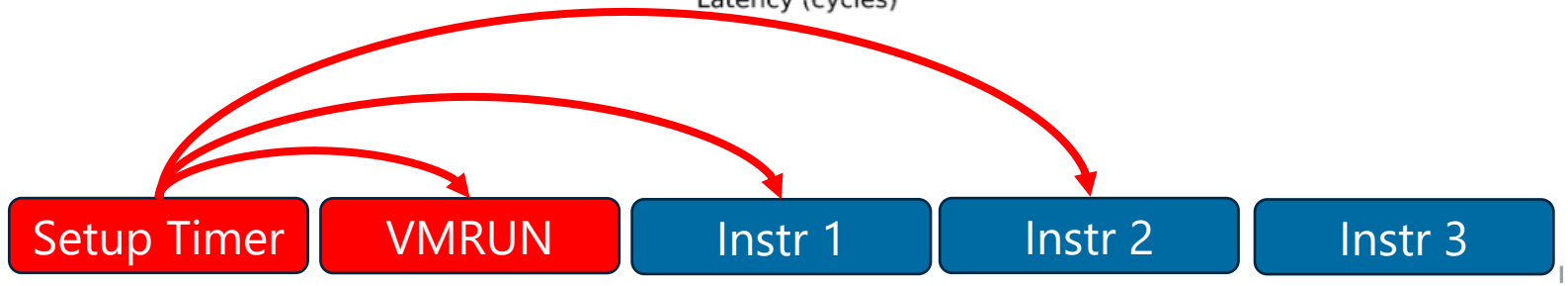
Single-Stepping: Naive Implementation



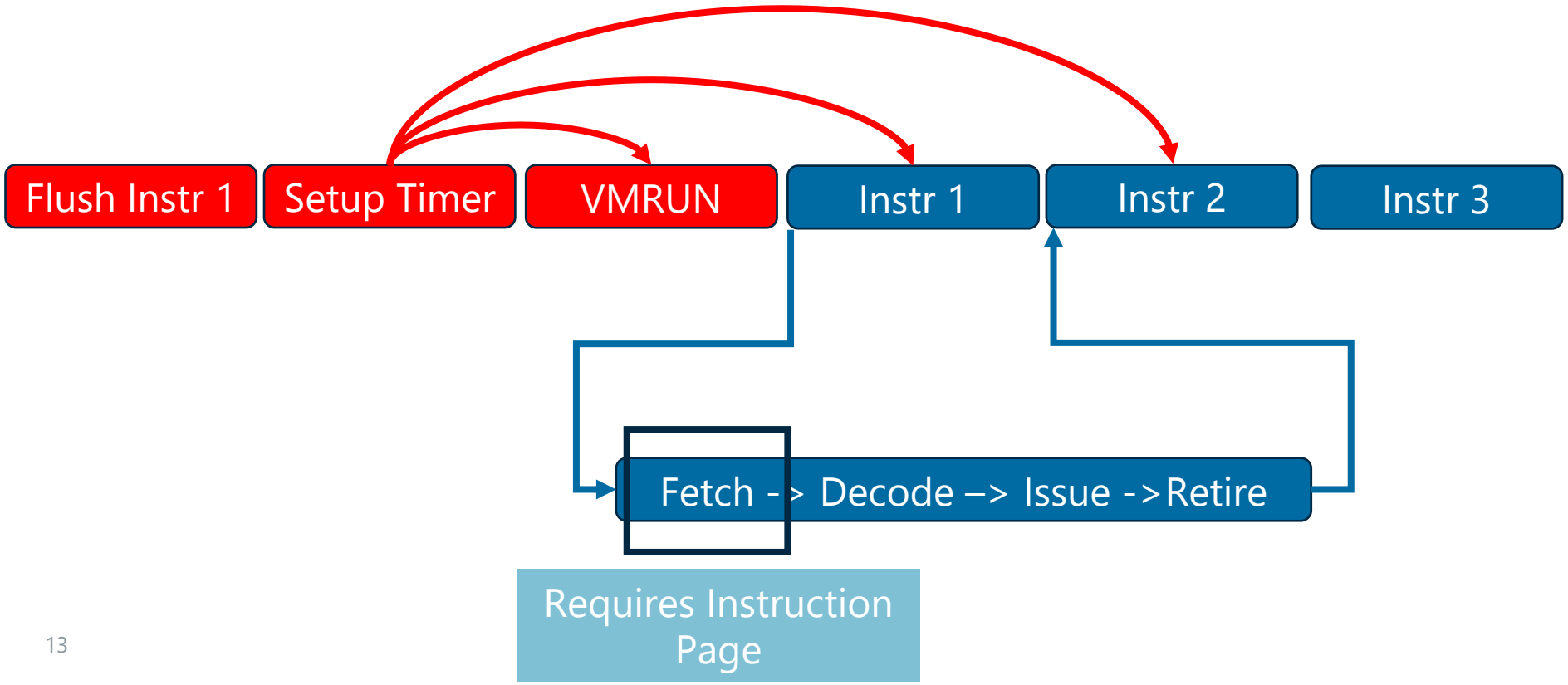
Single-Stepping: APIC Timing on SGX



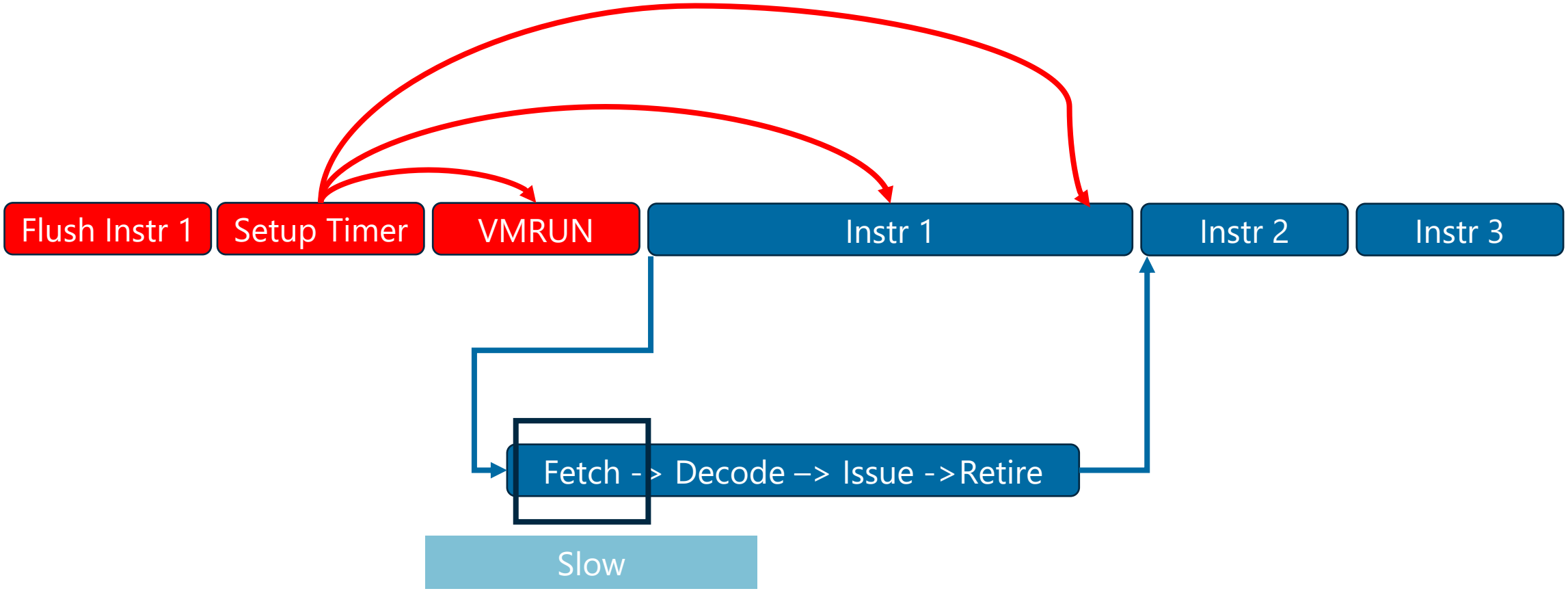
Measurements from AEX-Notify paper



Single-Stepping: Enlarge the Window



Single-Stepping: Enlarge the Window



SEV-Step

Design Goals, Implementation, Ongoing work

SEV-Step: Design Goals

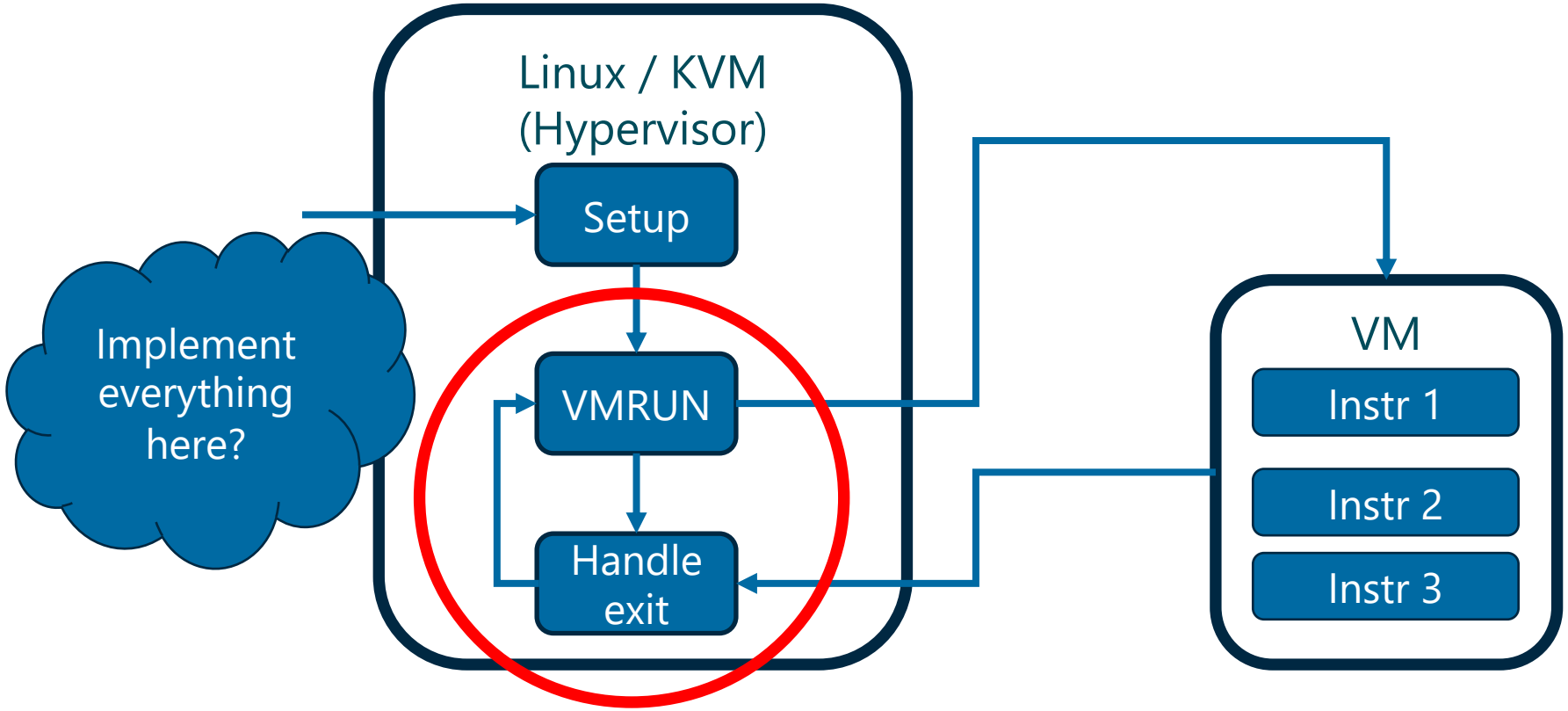
Reusability

- Separate primitives from attack logic

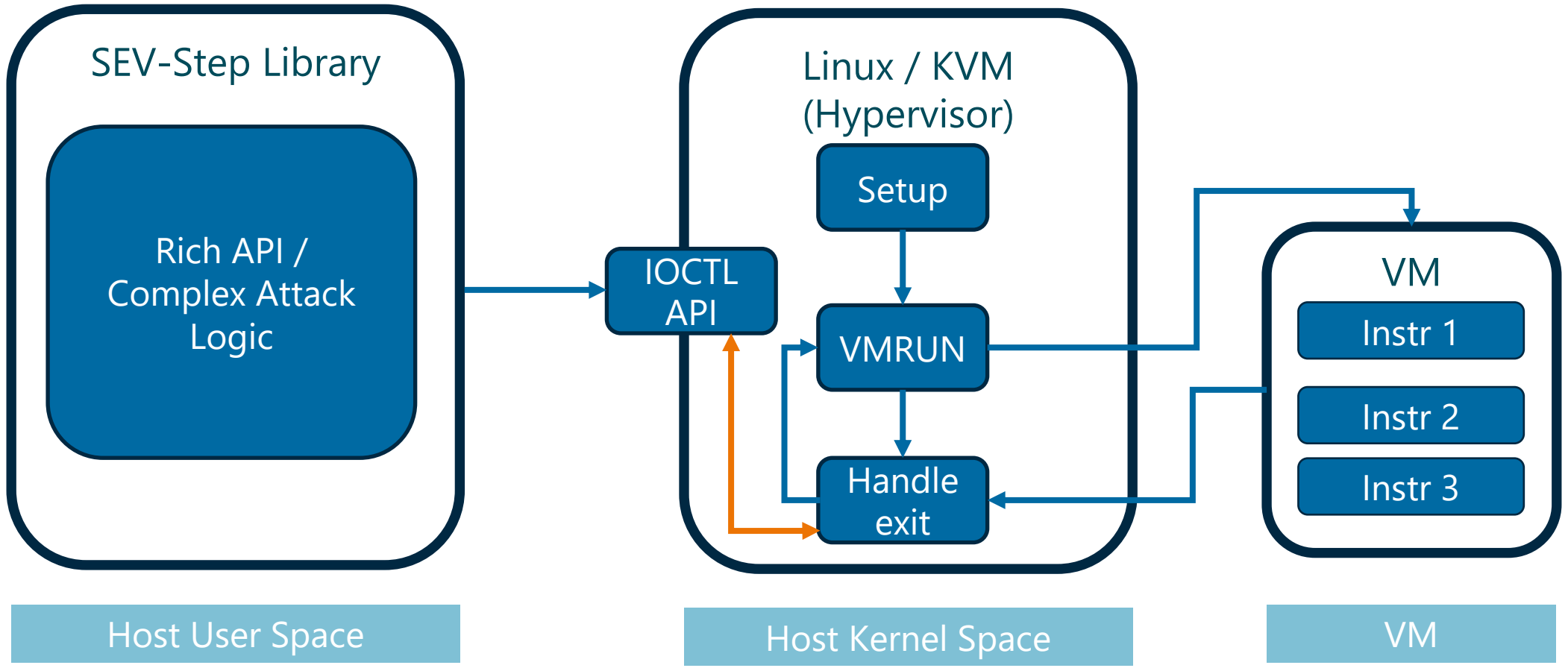
Interactivity

- Bidirectional Communication

SEV-Step: Reusability



SEV-Step: Reusability



SEV-Step: Design Goals

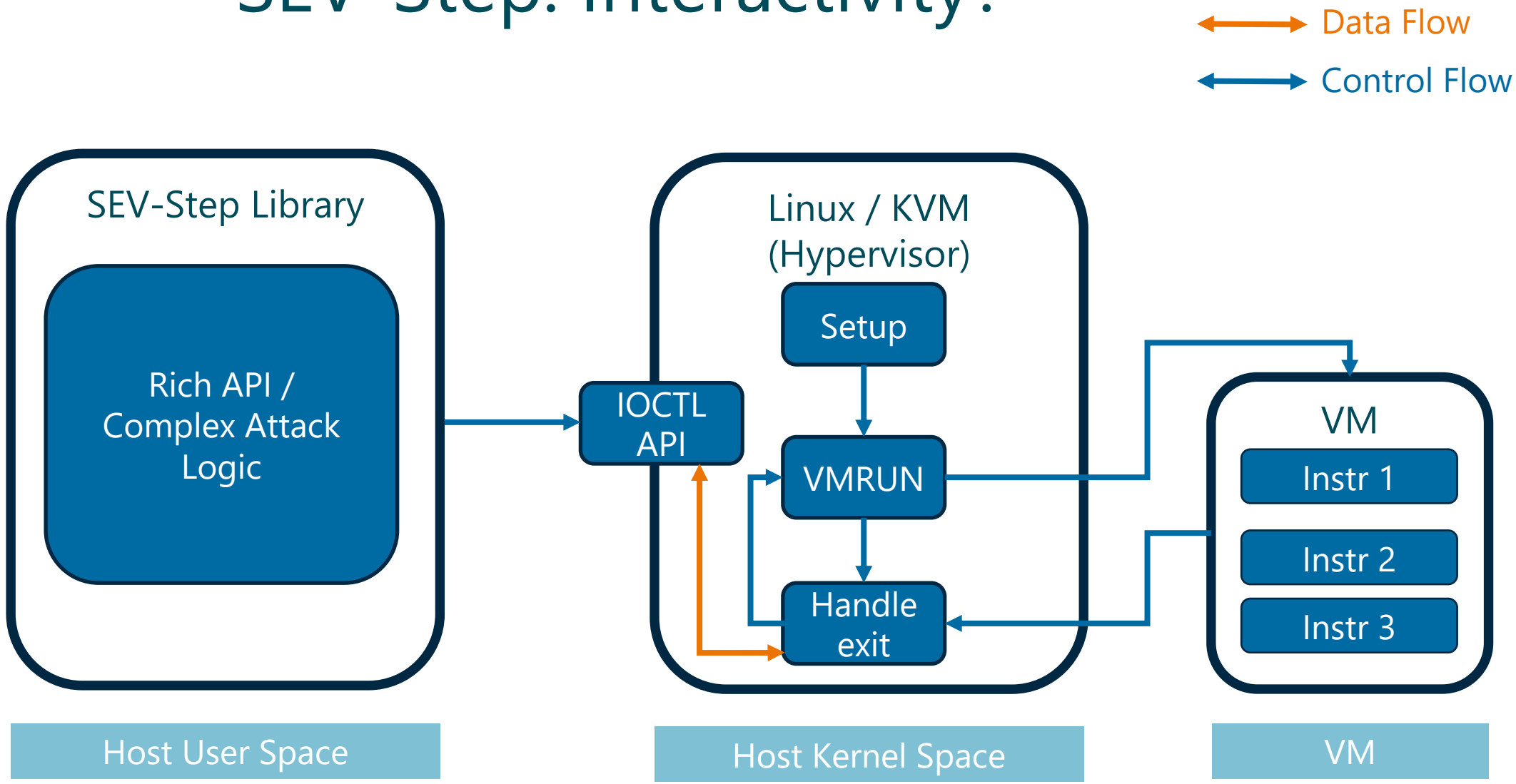
Reusability ✅

- Separate primitives from attack logic

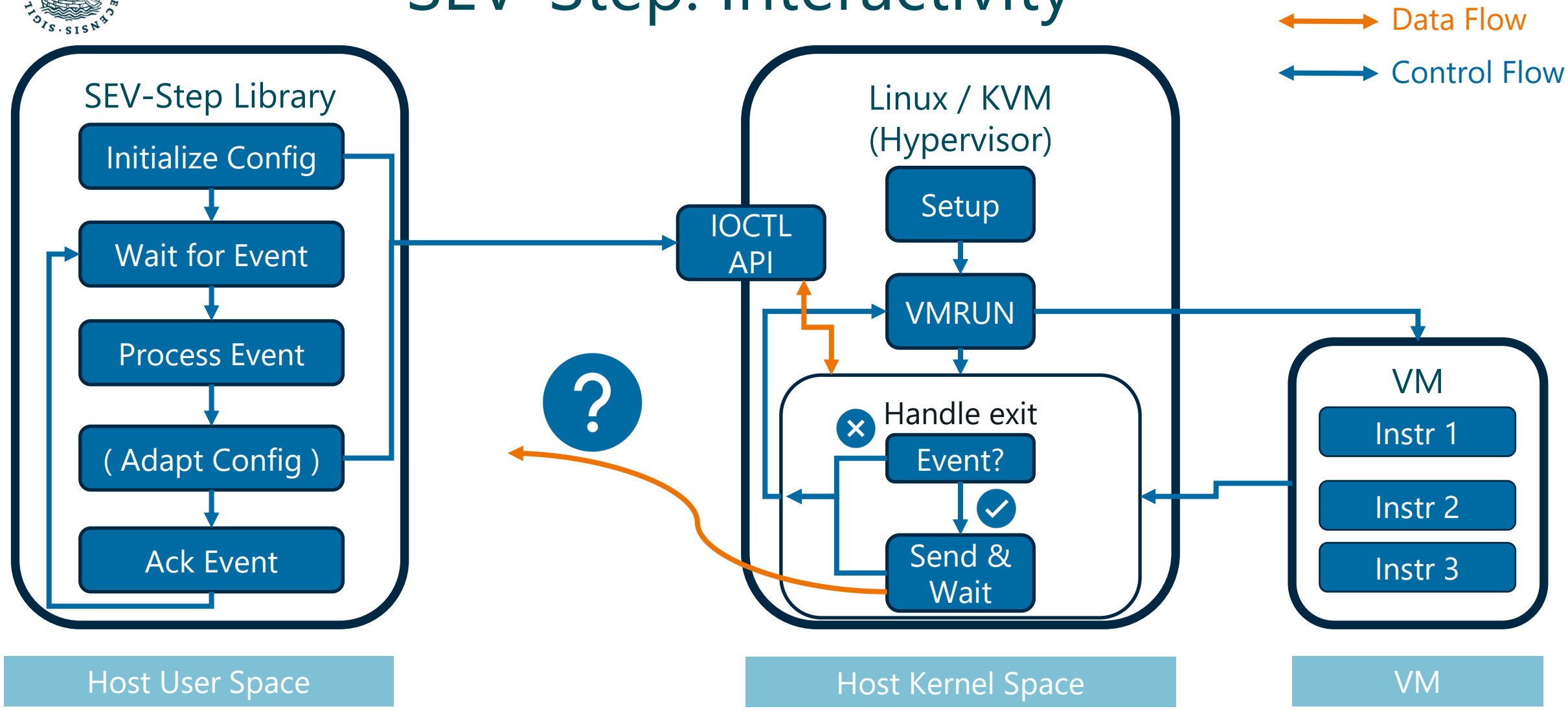
Interactivity

- Bidirectional Communication

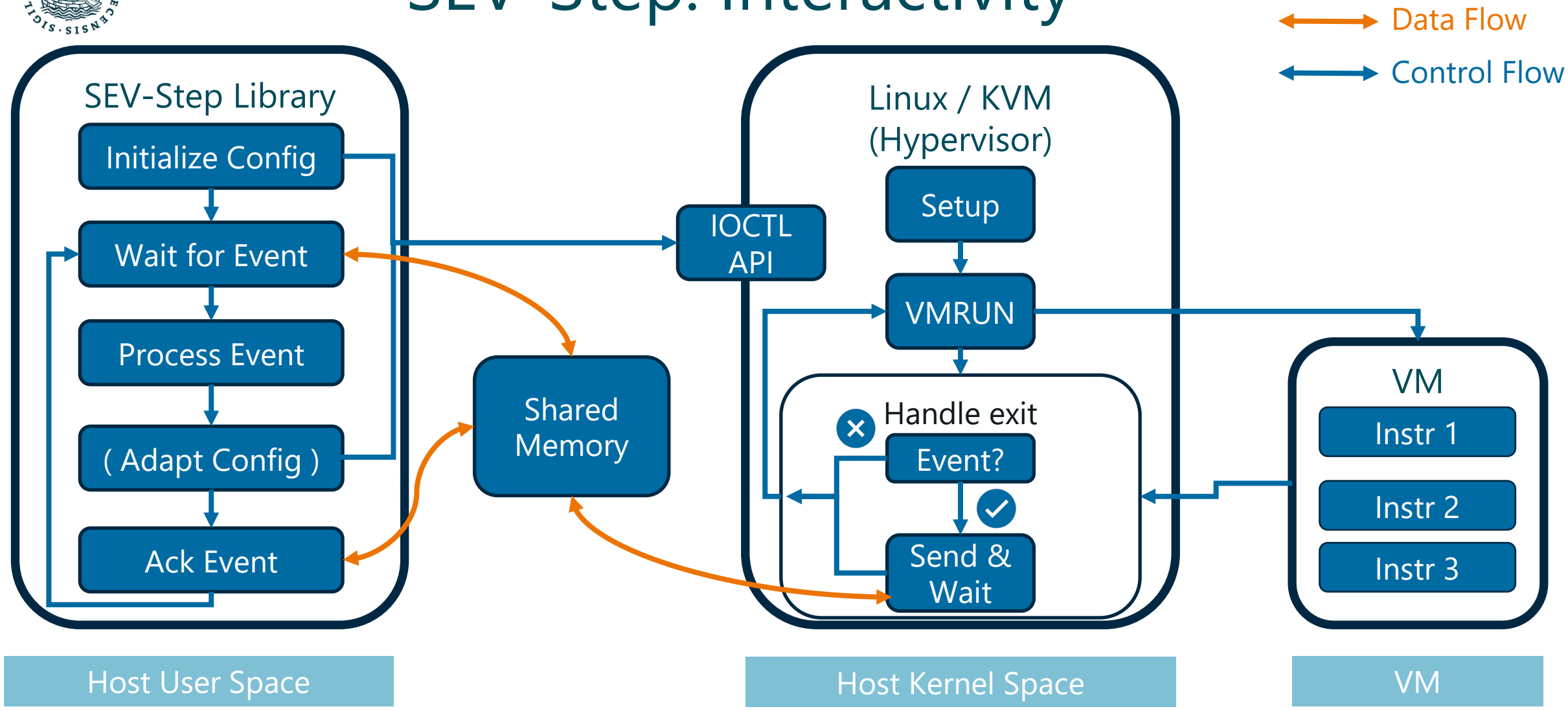
SEV-Step: Interactivity?



SEV-Step: Interactivity



SEV-Step: Interactivity



SEV-Step: Design Goals

Reusability ✅

- Separate primitives from attack logic

Interactivity ✅

- Bidirectional Communication

SEV-Step: Ongoing Work

- Improve API
  - Current Design: Track/Untrack, Start Stepping/Stop Stepping
  - Goal: High Level Components: „Track Pagefault Sequence“
  - Model SEV-Step + SGX-Step as „drivers“

Summary

- Single-Stepping enables many attacks
- Popularized for SGX with SGX-Step
- SEV-Step Framework
  - First to show that SEV is vulnerable to single-stepping
  - Ease attack research on SEV
  - GPL V2
- Ongoing work
  - Improve attack prototyping
- Play with it, break it, Improve it

SEV-Step

SGX-Step