RTLola: Formal Monitoring for CPS

Jan Baumeister

STREAM-BASED MONITORING

System   Monitor   Health
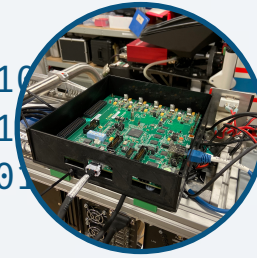
RTLola
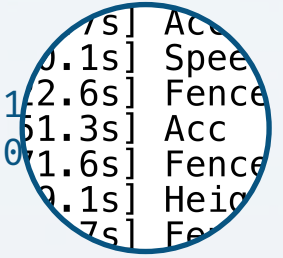
Formal Guarantees   Expressiveness

Specification Logics   Programming Languages

‣ Fully Formalized Semantic
‣ Strong Type System
‣ Strict Static Guarantees:
   ‣ Bounded Runtime Per Event
   ‣ Static Memory Bound Per Stream

FRAMEWORK
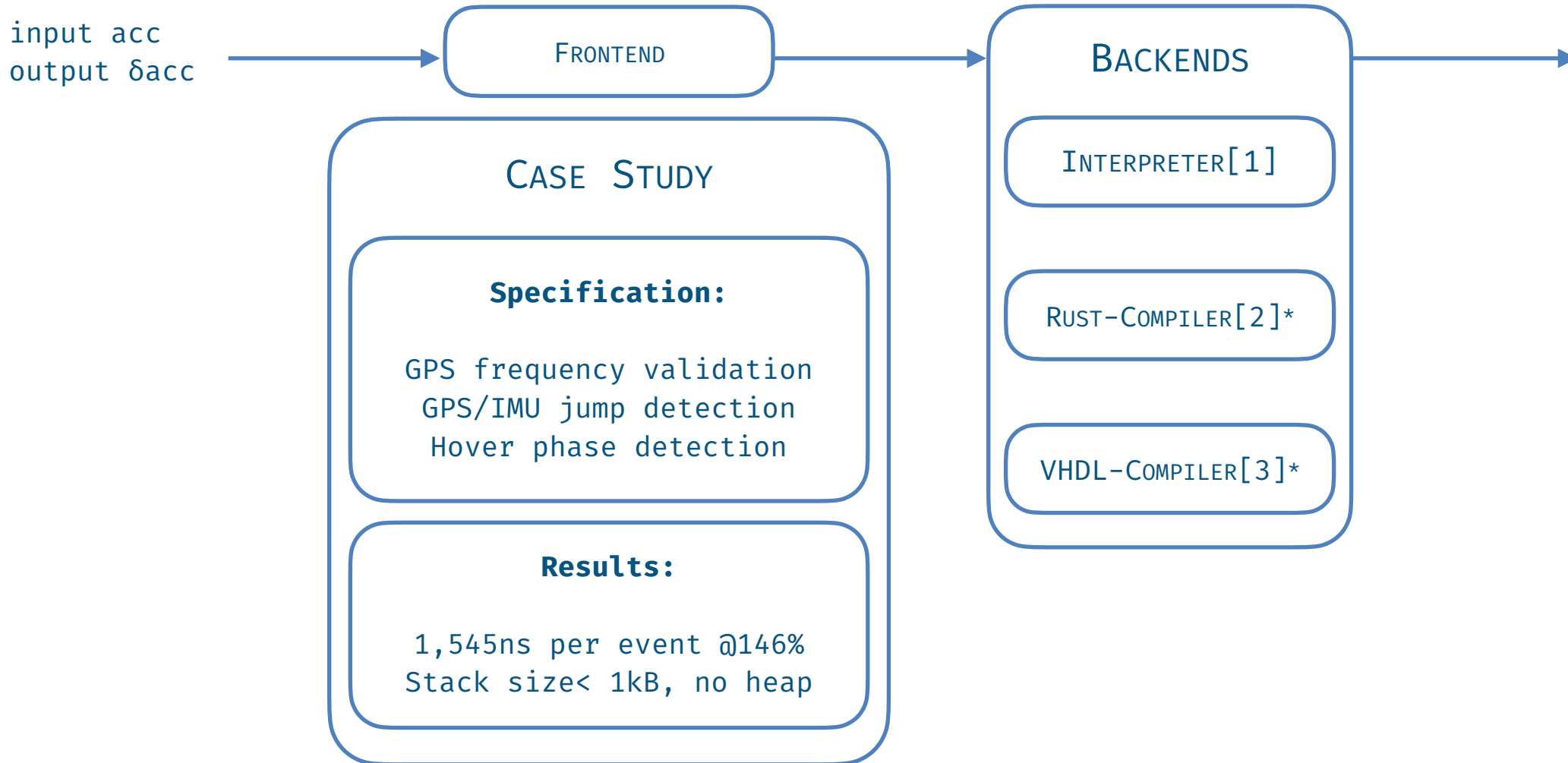
CISPA
HELMHOLTZ CENTER FOR
INFORMATION SECURITY

input acc
output δacc → FRONTEND → BACKENDS →

CASE STUDY

Specification:

GPS frequency validation
GPS/IMU jump detection
Hover phase detection

Results:

1,545ns per event @146%
Stack size< 1kB, no heap

BACKENDS

INTERPRETER[1]

RUST-COMPILER[2]*

VHDL-COMPILER[3]*

[1] StreamLAB: Stream-based Monitoring of Cyber-physical Systems@CAV19
[2] Verified Rust Monitors for Lola Specifications@RV20
[3] FPGA Stream-Monitoring of Real-time Properties@Emsoft19

- RTLoLA: expressive language with static analyses ensuring a safe integration

- Open source framework

- Successful integration in an UAS

www.rtlola.org