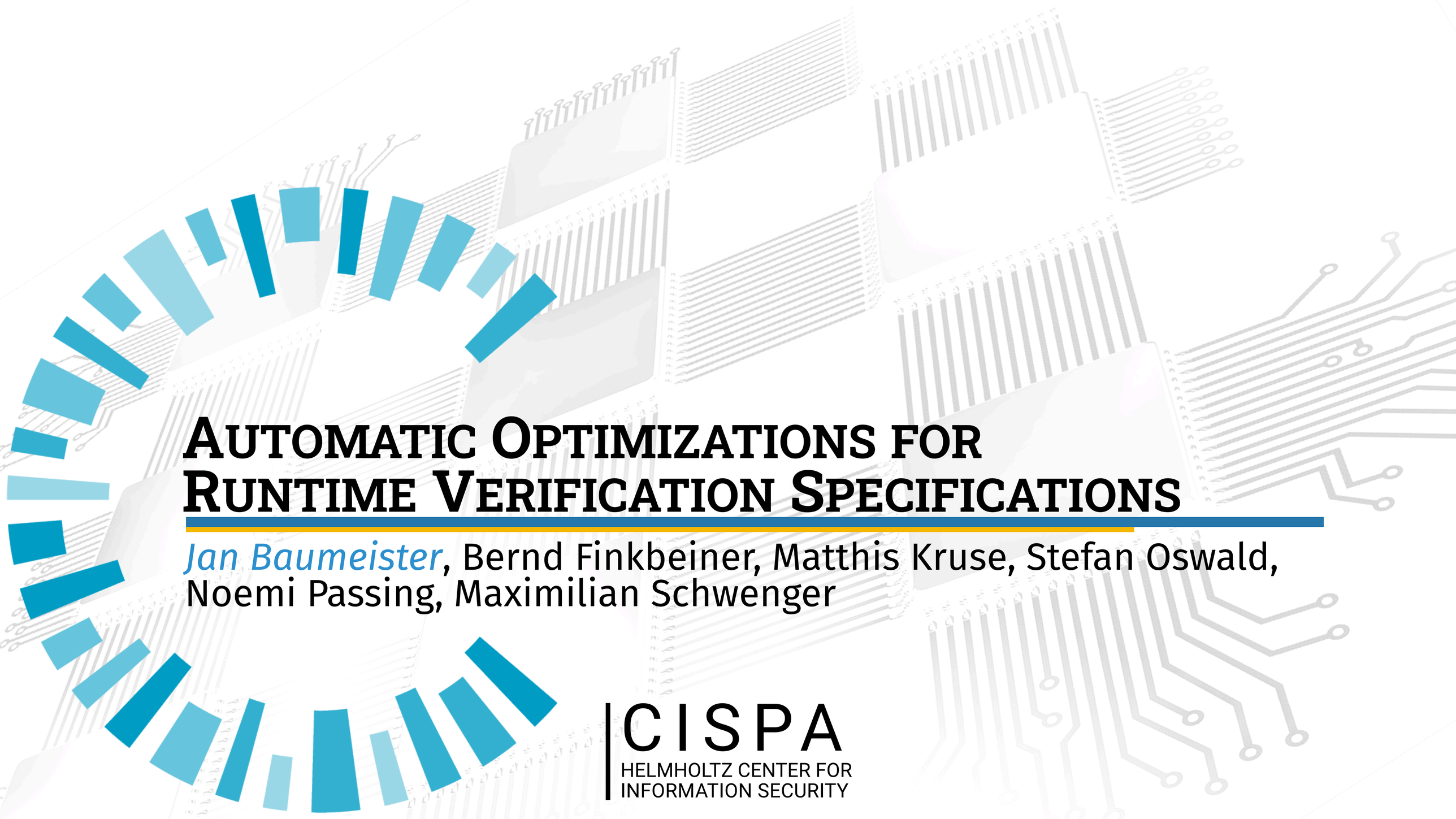


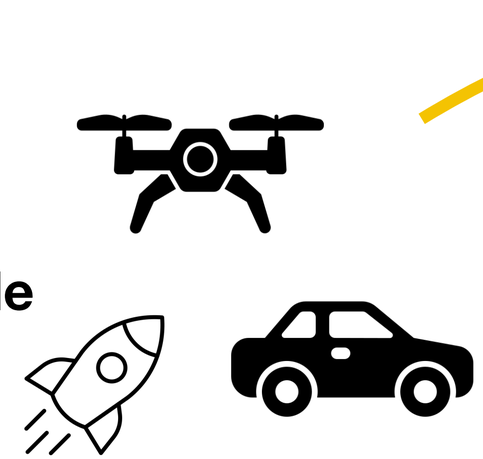
Automatic Optimizations for Runtime Verification Specifications

Jan Baumeister, Bernd Finkbeiner, Matthis Kruse, Stefan Oswald, Noemi Passing, Maximilian Schwenger

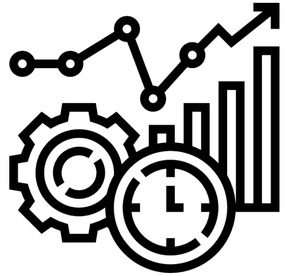
CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

Motivation

safety-critical
understandable
code

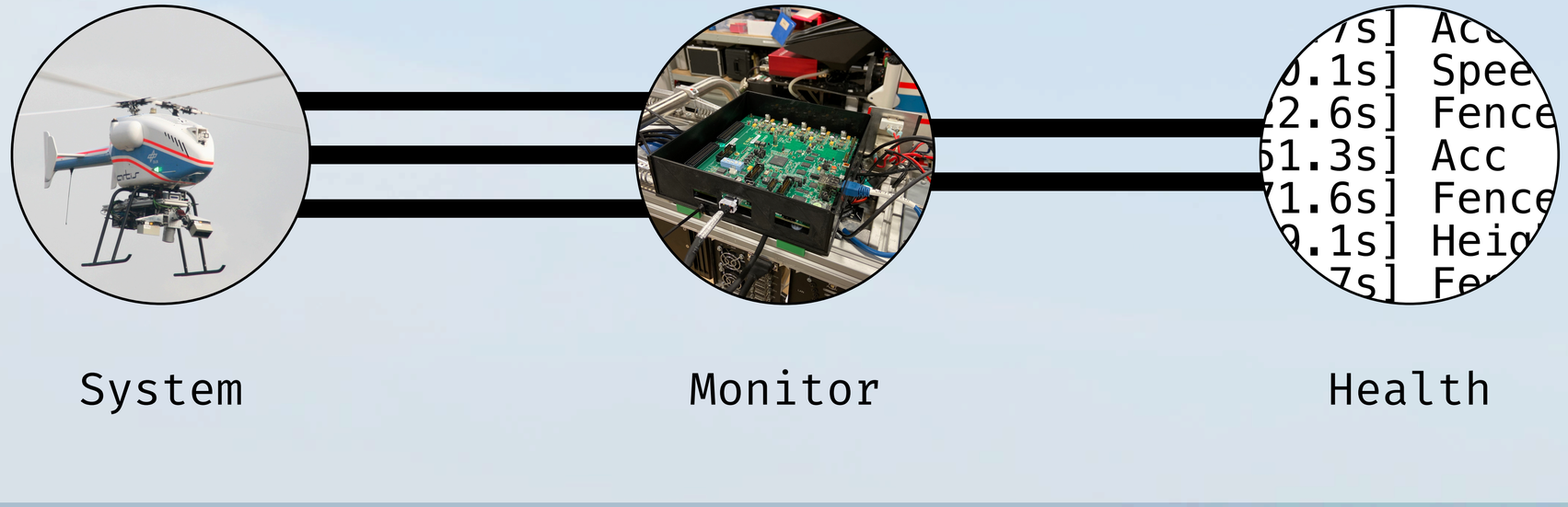


Optimizations



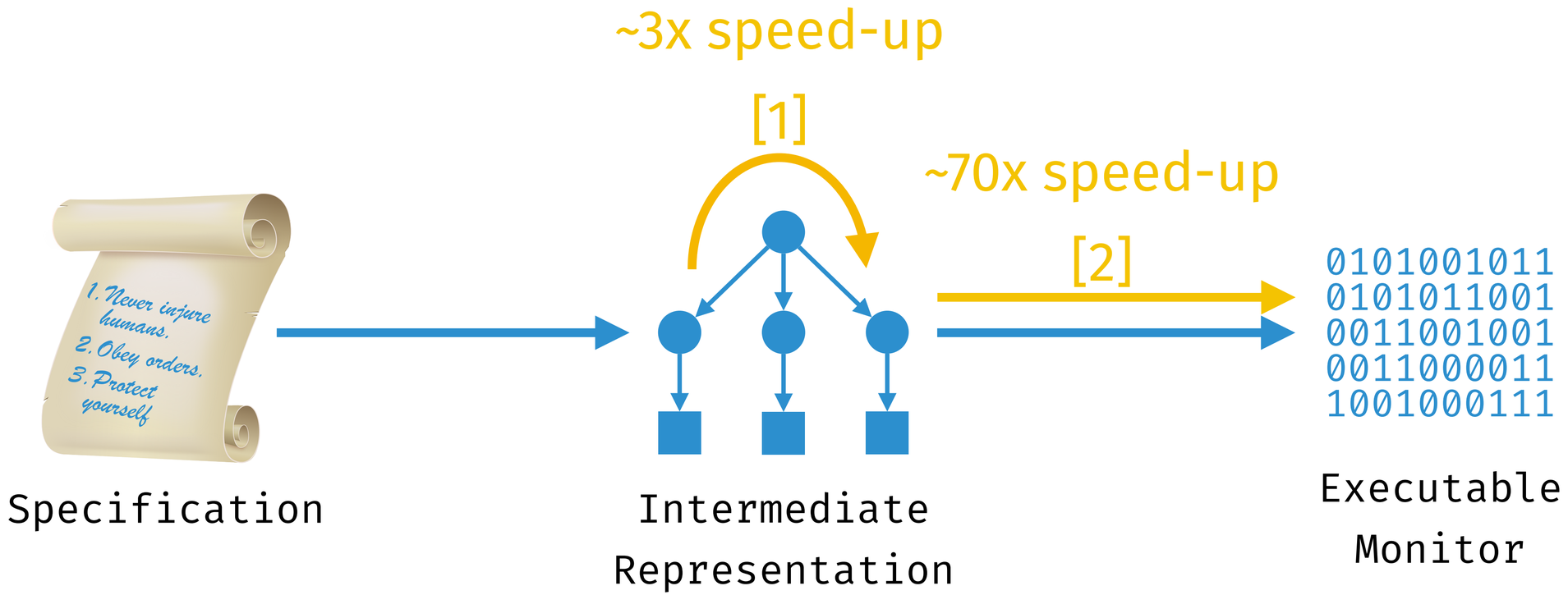
real-time
efficient
execution

LOLA / RTLOLA



RTLola Cleared for Take-Off: Monitoring Autonomous Aircraft. CAV 2020

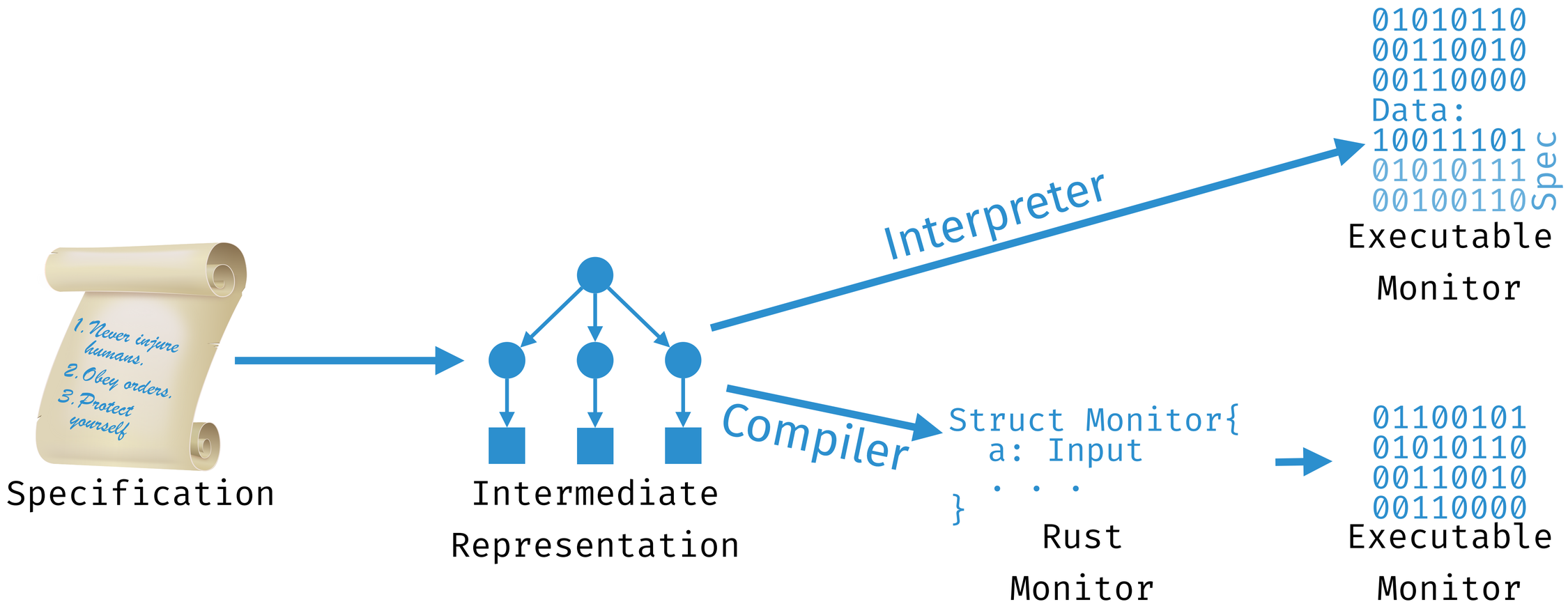
Overview



[1] Automatic Optimizations for Stream-based Monitoring Languages. RV 2020

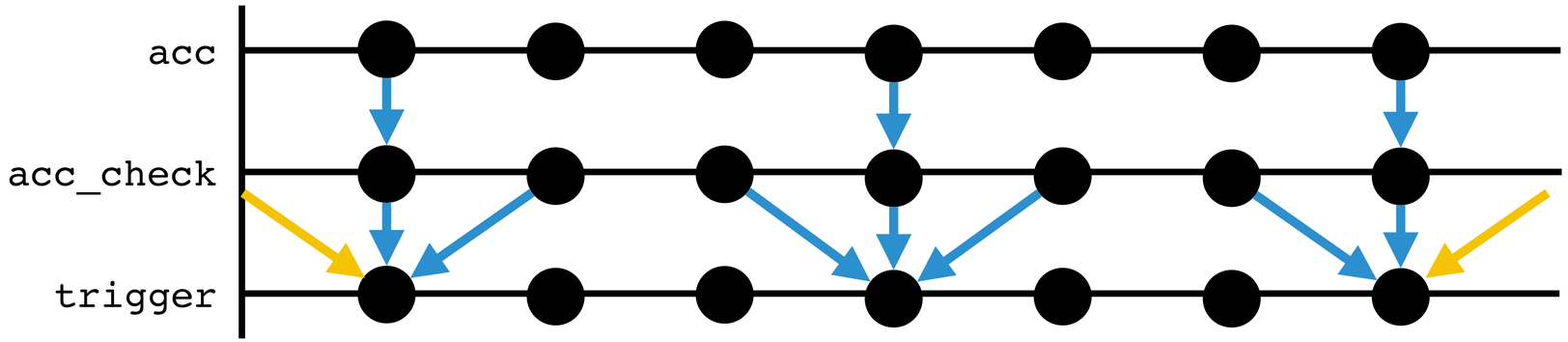
[2] Verified Rust Monitors for Lola Specifications. RV 2020

Interpreter v. Compiler



LOLA BY EXAMPLE

```
input acc: Float64
```



Three Phases

I. Eradicate Most Conditionals
II. Replace Memory Accesses with Constants

```
fn prefix() {
   false
   ∧ check_acc0
   ∧ check_acc+1
}
```

Prefix

```
while let Some(…)
     = get_input() {
   if pos > 0 then check_acc-1
   check_acc-1 else false
   ∧ check_acc0
   ∧ if pos > 0 then check_acc+1
                else false
}
```

Monitor Loop

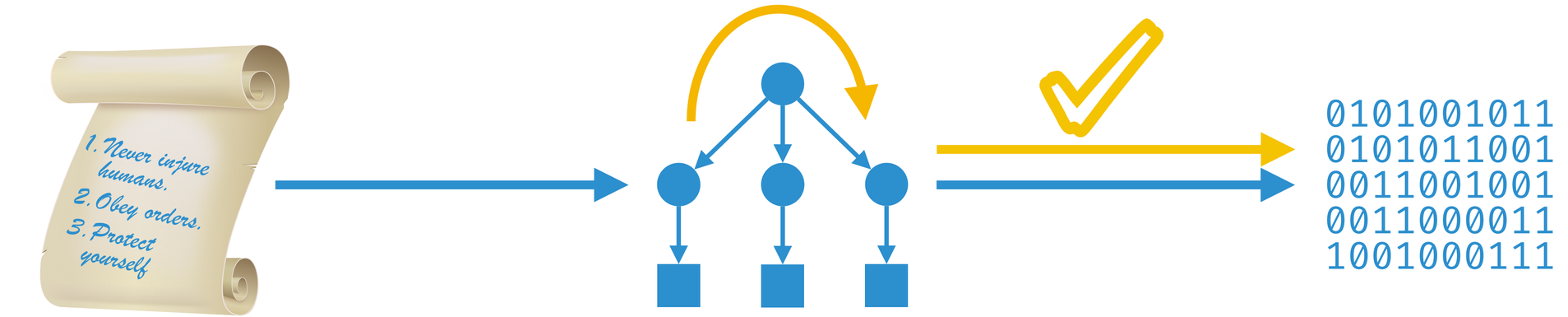
```
fn postfix() {
 check_acc-1
   ∧ check_acc0
   ∧ false
}
```

Postfix

Evaluation

Interpreter	438ns	1.535µs
Compilation	6ns (73 x speed up)	63ns (~24 x speed up)

Overview



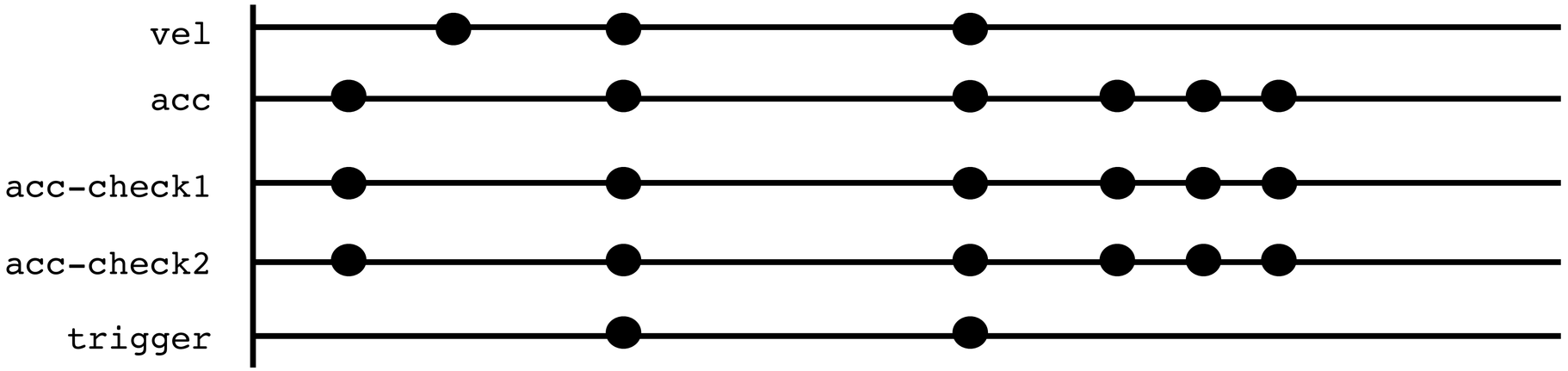
Specification

Intermediate Representation

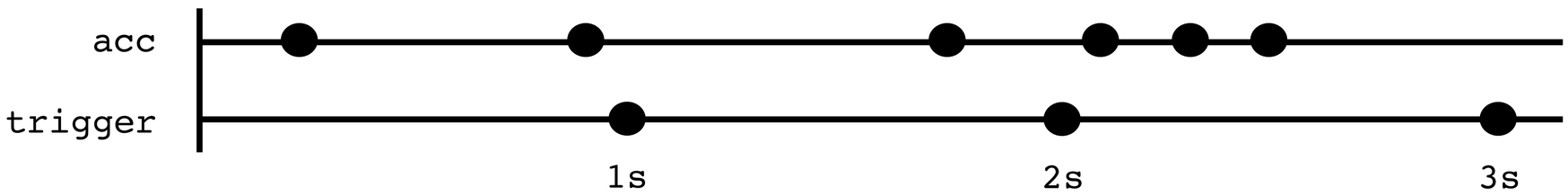
Executable Monitor

LOLA v. RTLOLA

Asynchrony



Real-time



RTLola by Example

- If the current velocity is above 10 m/s, the acceleration must stay below 1 m/s^2
- Otherwise an acceleration of up to 1.5 m/s^2 is possible

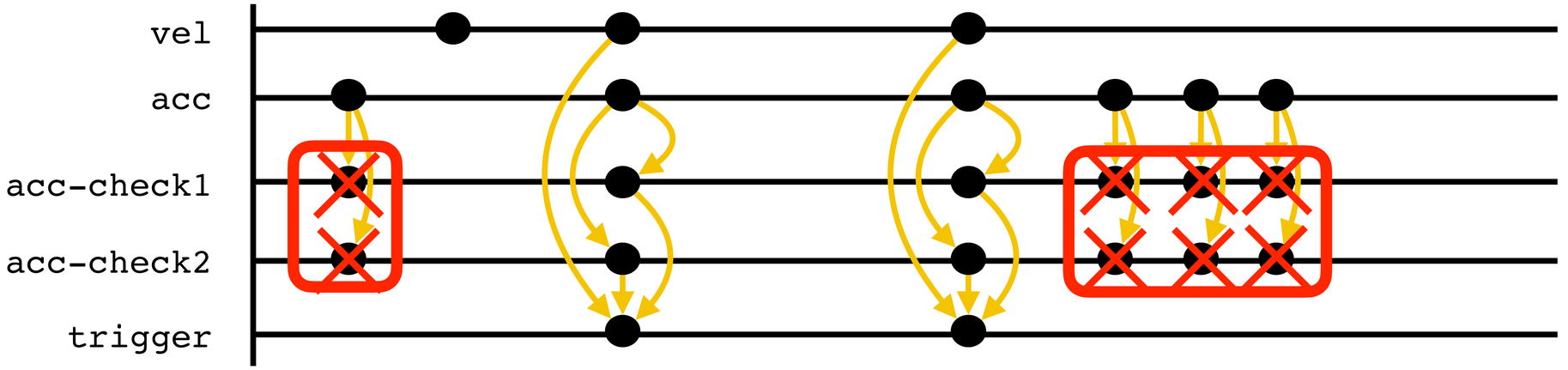
```
input acc: Float64
input vel: Float64
```

Pacing Types

STATIC ELIMINATION OF UNNECESSARY COMPUTATIONS

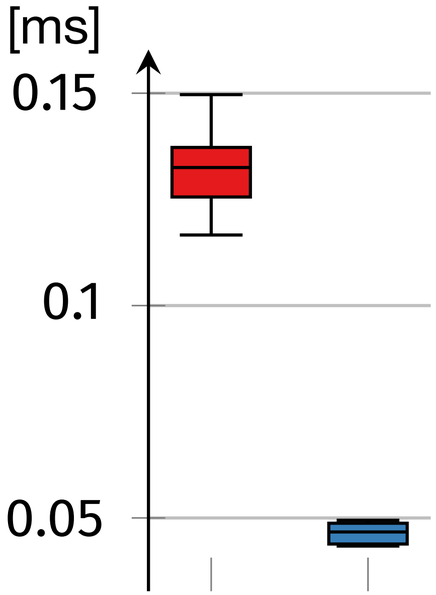
```
input acc: Float64
input vel: Float64
output acc_check_1 := acc < 1.0
output acc_check_2 := acc < 1.5
trigger if vel < 10.0 then acc_check_1 else acc_check_2
```

vel∧acc



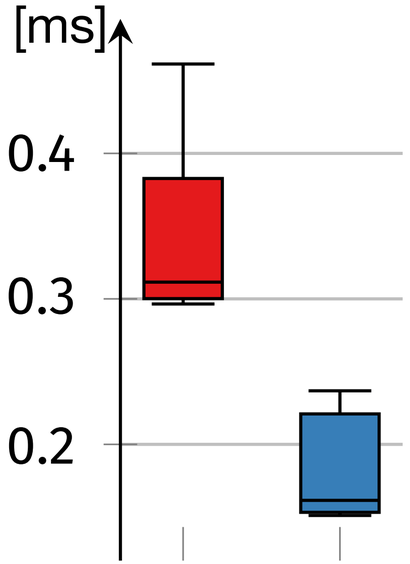
Evaluation

Pacing Type Refinement



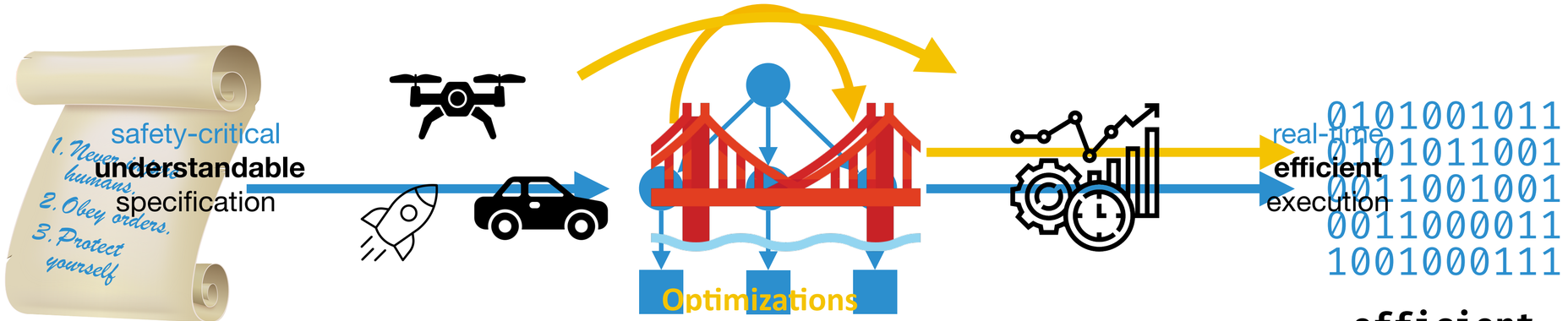
3x speed up

Sparse Conditional Constant Propagation



2x speed up

Conclusion



understandable

Specification

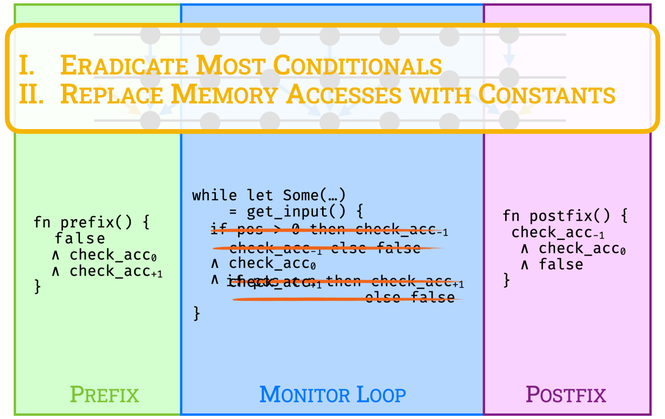
efficient

Executable

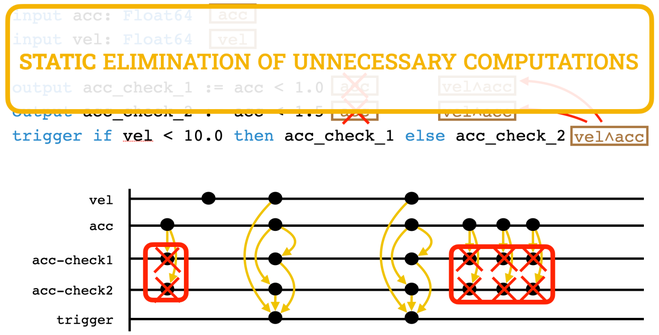
Monitor

www.rtlola.org

Three Phases



7



12