The MoXI Model Exchange Tool Suite

Chris Johannsen (1)
Karthik Nukala (2)
Rohit Dureja (3)
Ahmed Irfan (2)

(1) Iowa State University
(2) SRI International
(3) Advanced Micro Devices

Natarajan Shankar (2)
Cesare Tinelli (4)
Moshe Y. Vardi (5)
Kristin Yvonne Rozier (1)

(4) University of Iowa
(5) Rice University

IOWA STATE UNIVERSITY

The MoXI Model Exchange Tool Suite

Chris Johannsen (1)
Karthik Nukala (2)
Rohit Dureja (3)
Ahmed Irfan (2)

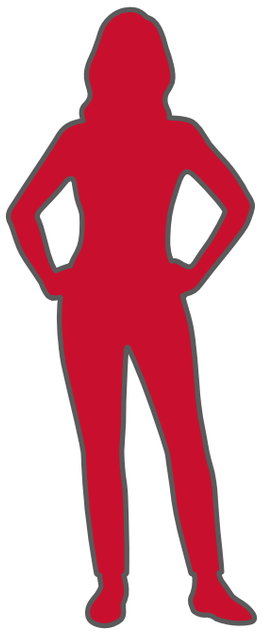
(1) Iowa State University
(2) SRI International
(3) Advanced Micro Devices

Natarajan Shankar (2)
Cesare Tinelli (4)
MoXI Y. Vardi (5)
Kristin Yvonne Rozier (1)

(4) University of Iowa
(5) Rice University

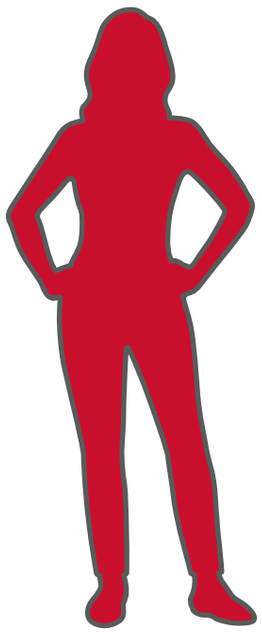
IOWA STATE UNIVERSITY

Mary the Model-Checking Researcher



$$M \models \varphi$$

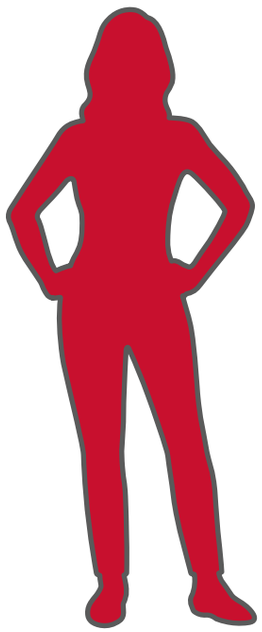
Mary the Model-Checking Researcher



$$M \models \varphi$$

- Algorithms
- Certificates
- …

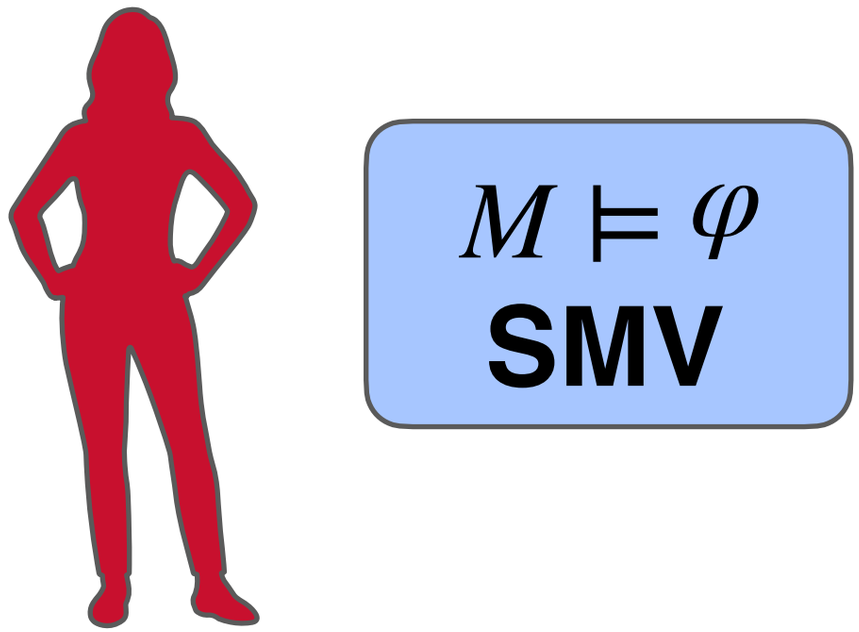
Mary the Model-Checking Researcher



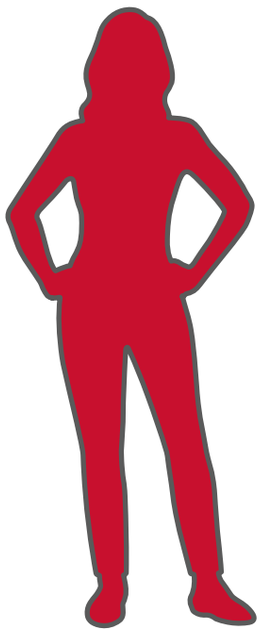
$$M \models \varphi$$

- **Algorithms**
- Certificates
- …

Mary the Model-Checking Researcher



Mary the Model-Checking Researcher

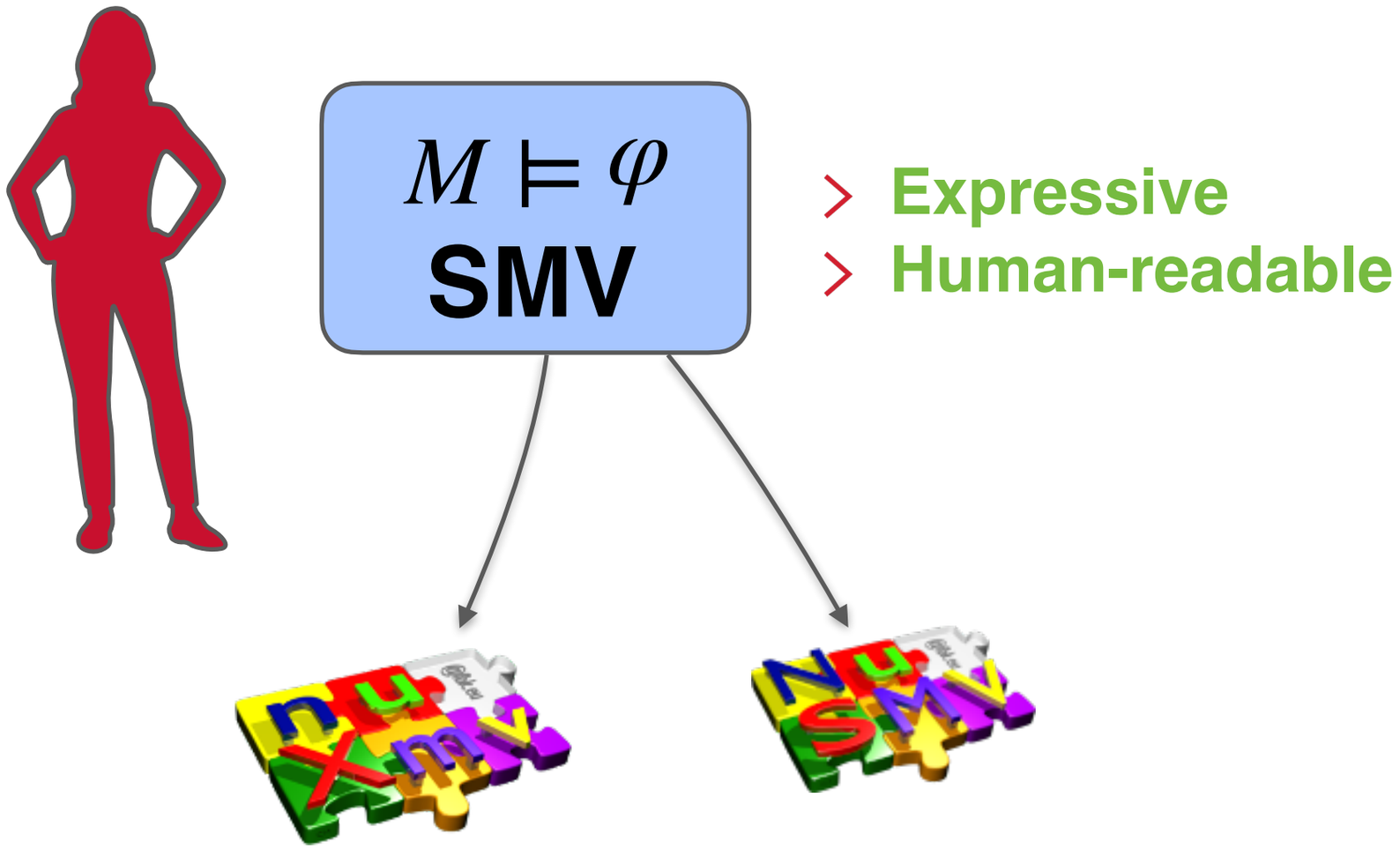


$M \models \varphi$

SMV

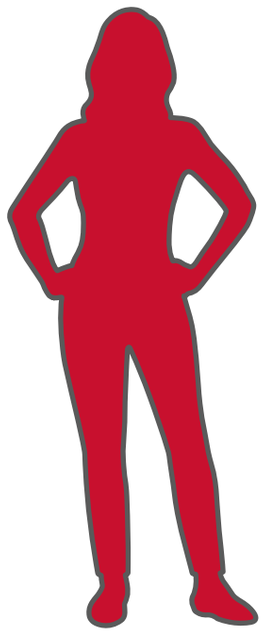
- **Expressive**
- **Human-readable**

Mary the Model-Checking Researcher



- Expressive
- Human-readable

Mary the Model-Checking Researcher



$M \models \varphi$

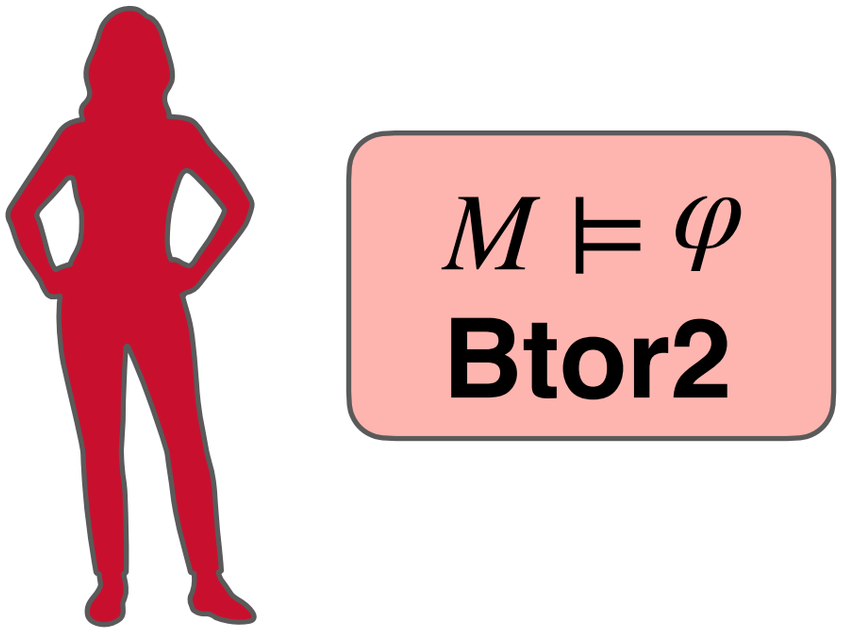
SMV

- **Expressive**
- **Human-readable**

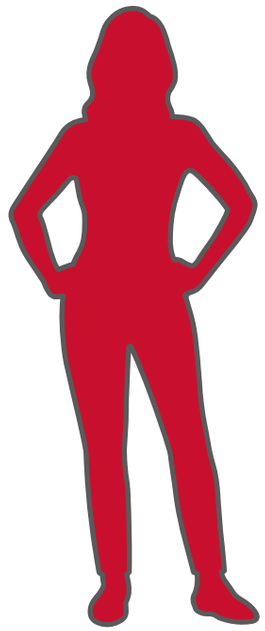
- **Closed-source**

- **Not state-of-the-art**

Mary the Model-Checking Researcher



Mary the Model-Checking Researcher

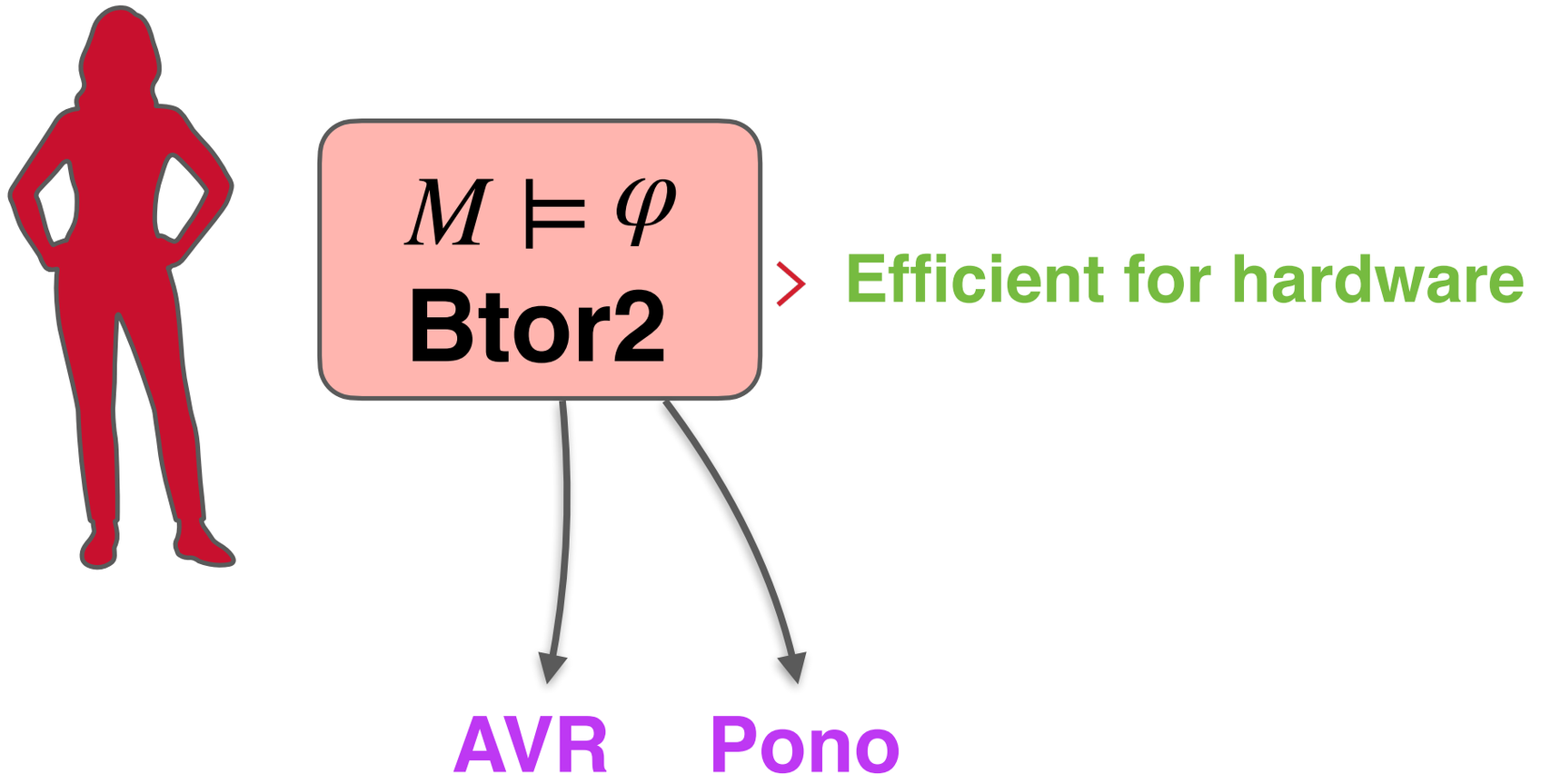


$M \models \varphi$

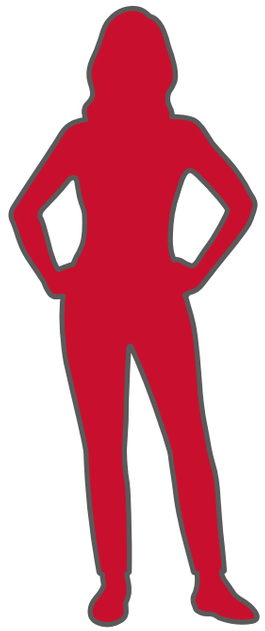
Btor2

> **Efficient for hardware**

Mary the Model-Checking Researcher



Mary the Model-Checking Researcher



$M \models \varphi$

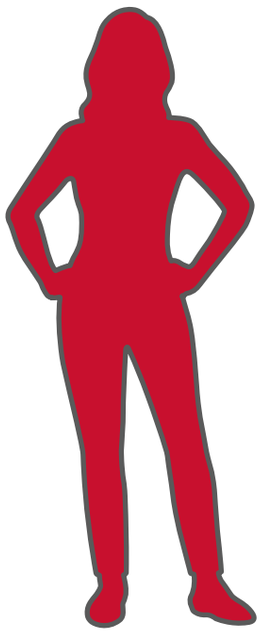
Btor2

- Efficient for hardware

AVR **Pono**

- Open-source
- State-of-the-art

Mary the Model-Checking Researcher



$M \models \varphi$

Btor2

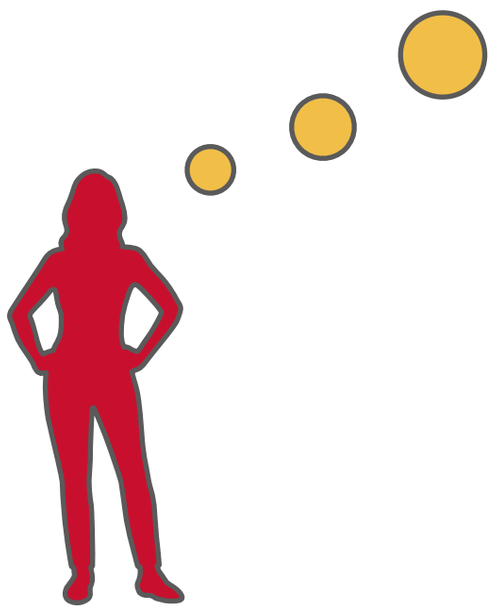
- **Efficient for hardware**
- **Limited modeling language**

AVR **Pono**

- **Open-source**
- **State-of-the-art**

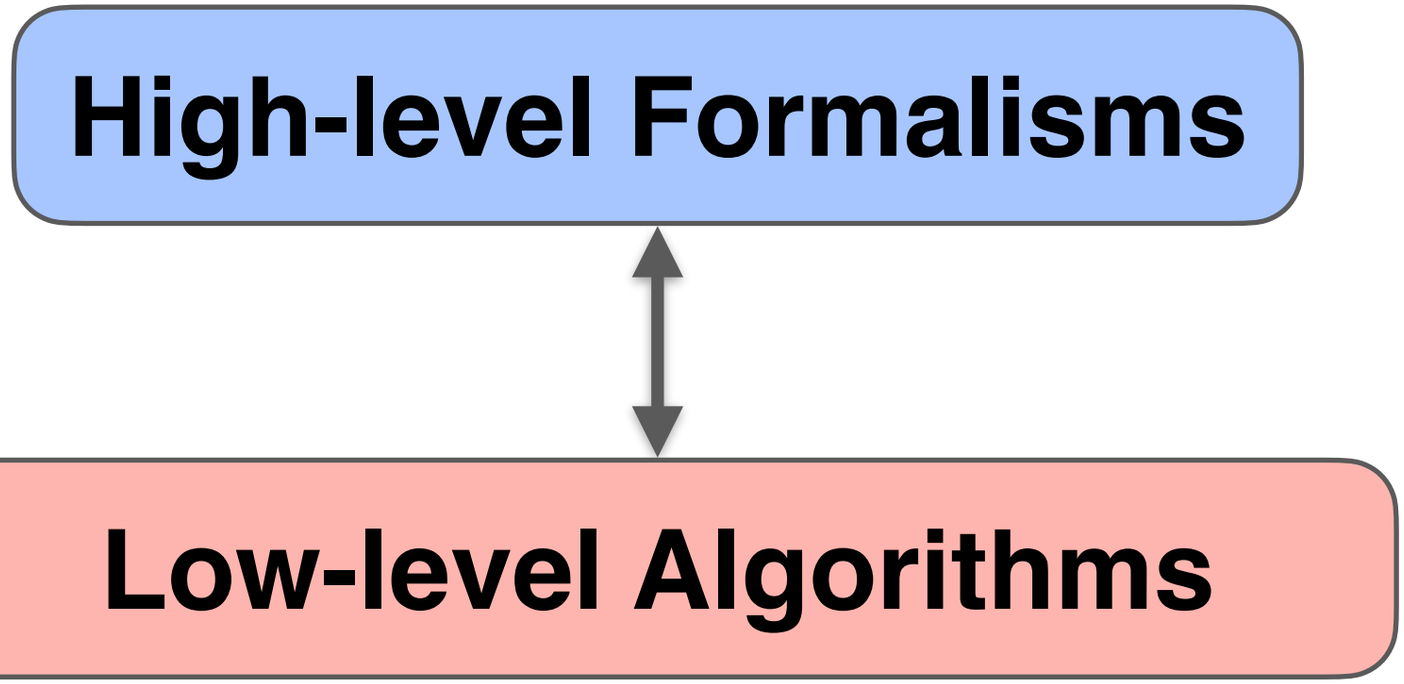
Mary the Model-Checking Researcher

- **High-level formalisms**
- **Low-level algorithms**
- **Open-source, state-of-the art tools**



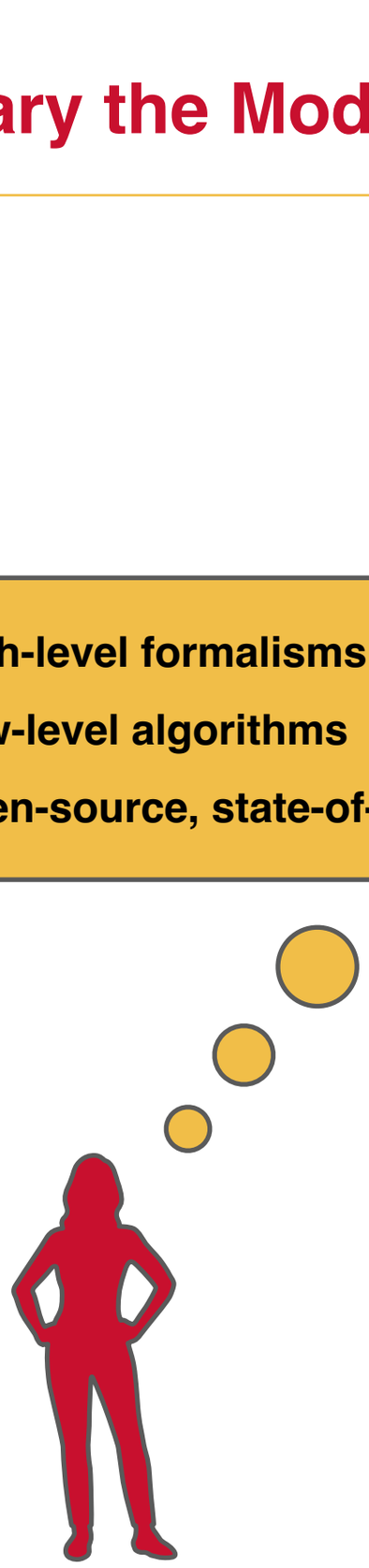
Mary the Model-Checking Researcher

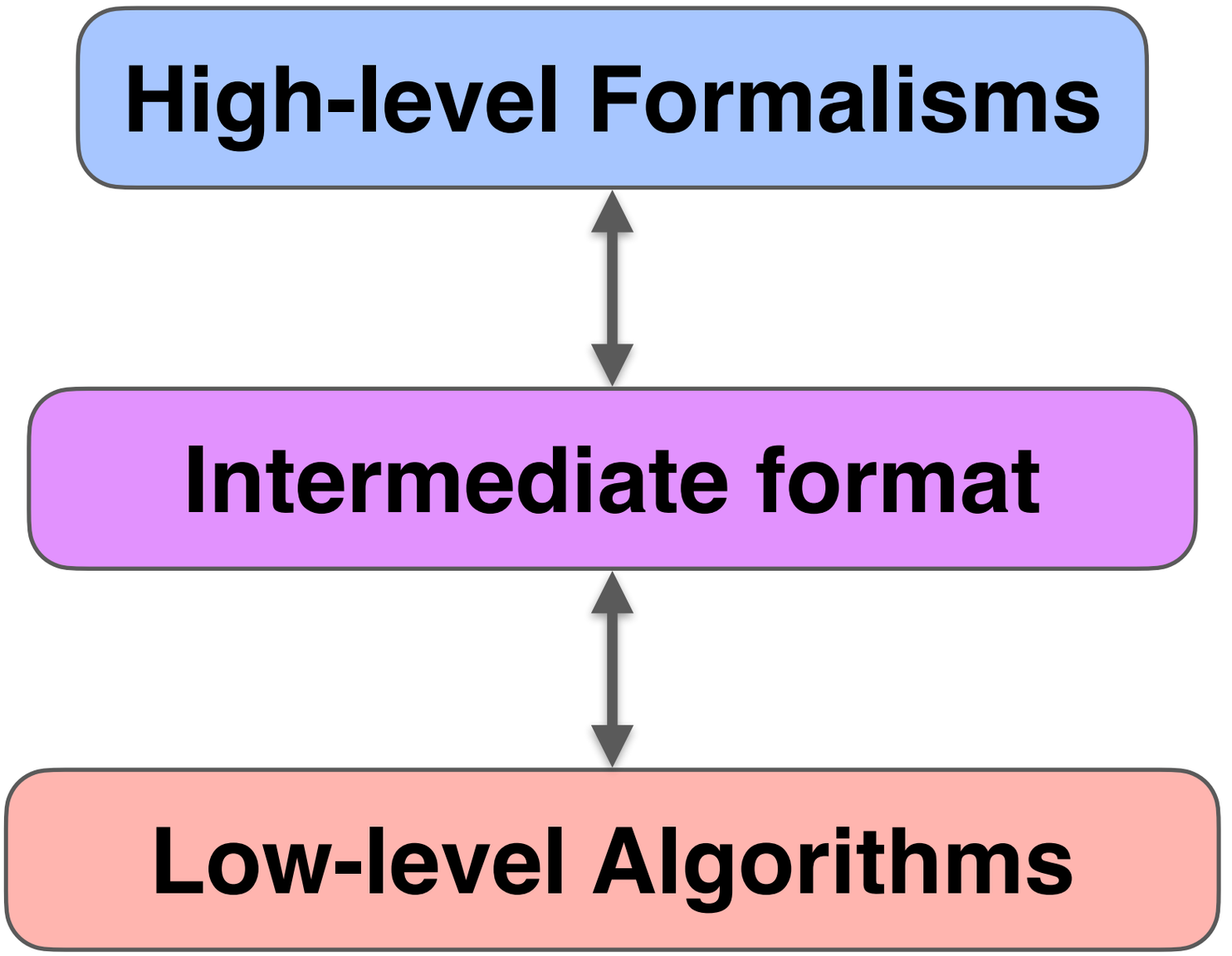
- High-level formalisms
- Low-level algorithms
- Open-source, state-of-the art tools



Mary the Model-Checking Researcher

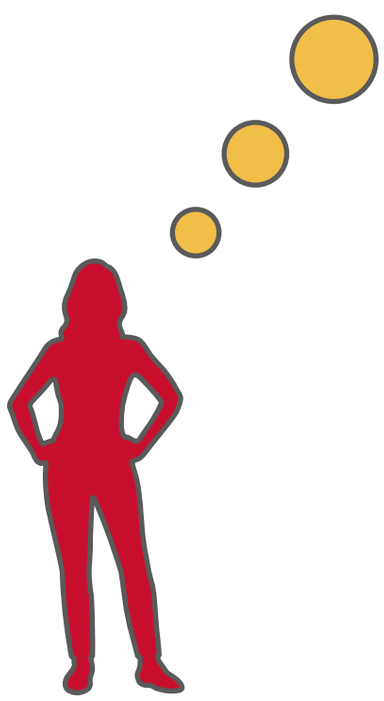
- High-level formalisms
- Low-level algorithms
- Open-source, state-of-the art tools

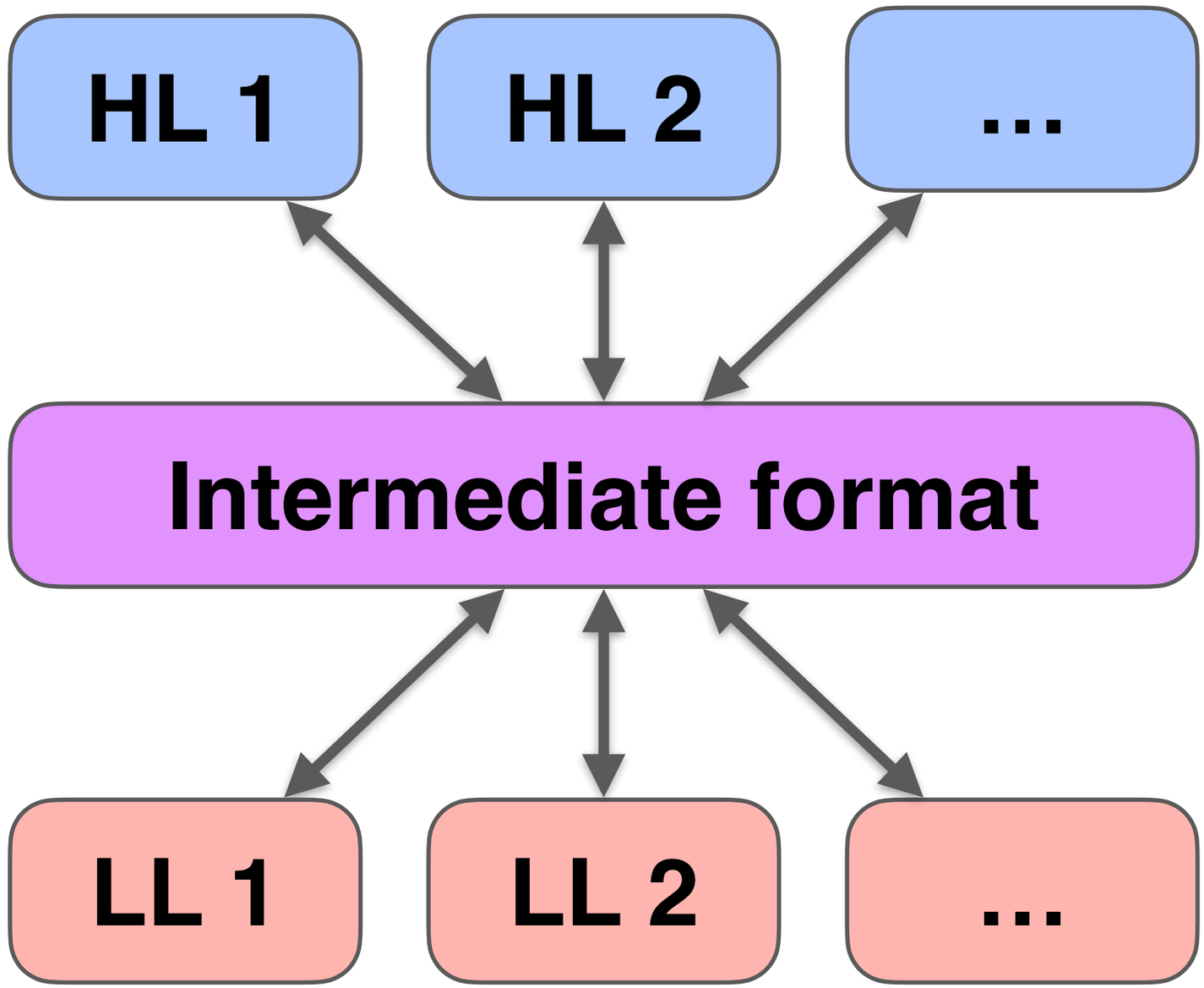




Mary the Model-Checking Researcher

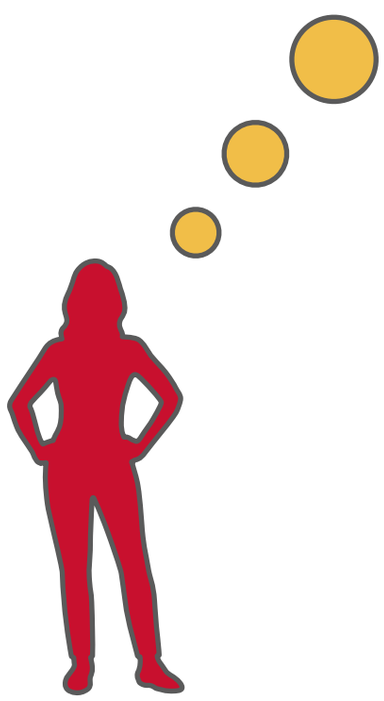
- High-level formalisms
- Low-level algorithms
- Open-source, state-of-the art tools

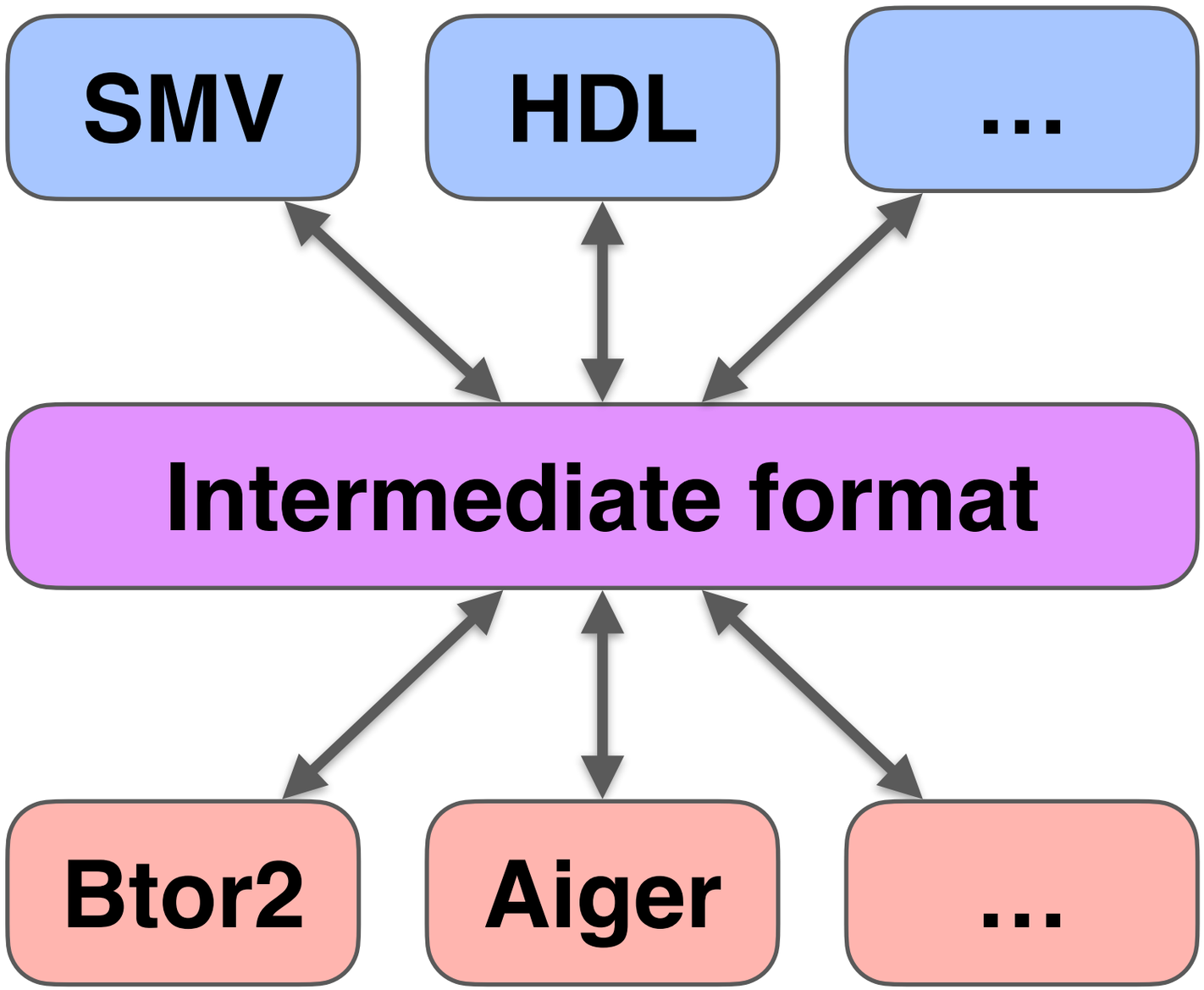




Mary the Model-Checking Researcher

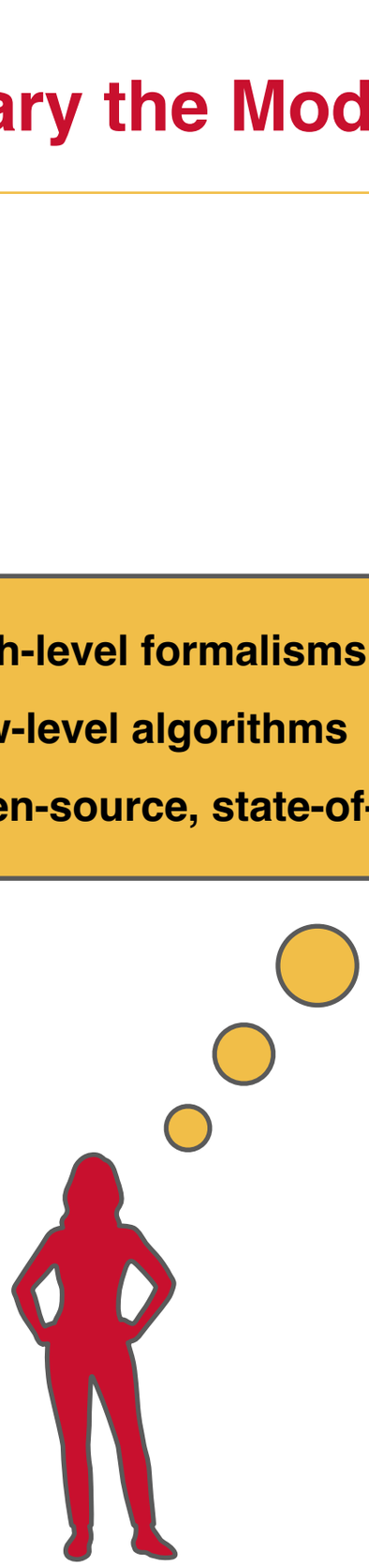
- High-level formalisms
- Low-level algorithms
- Open-source, state-of-the art tools

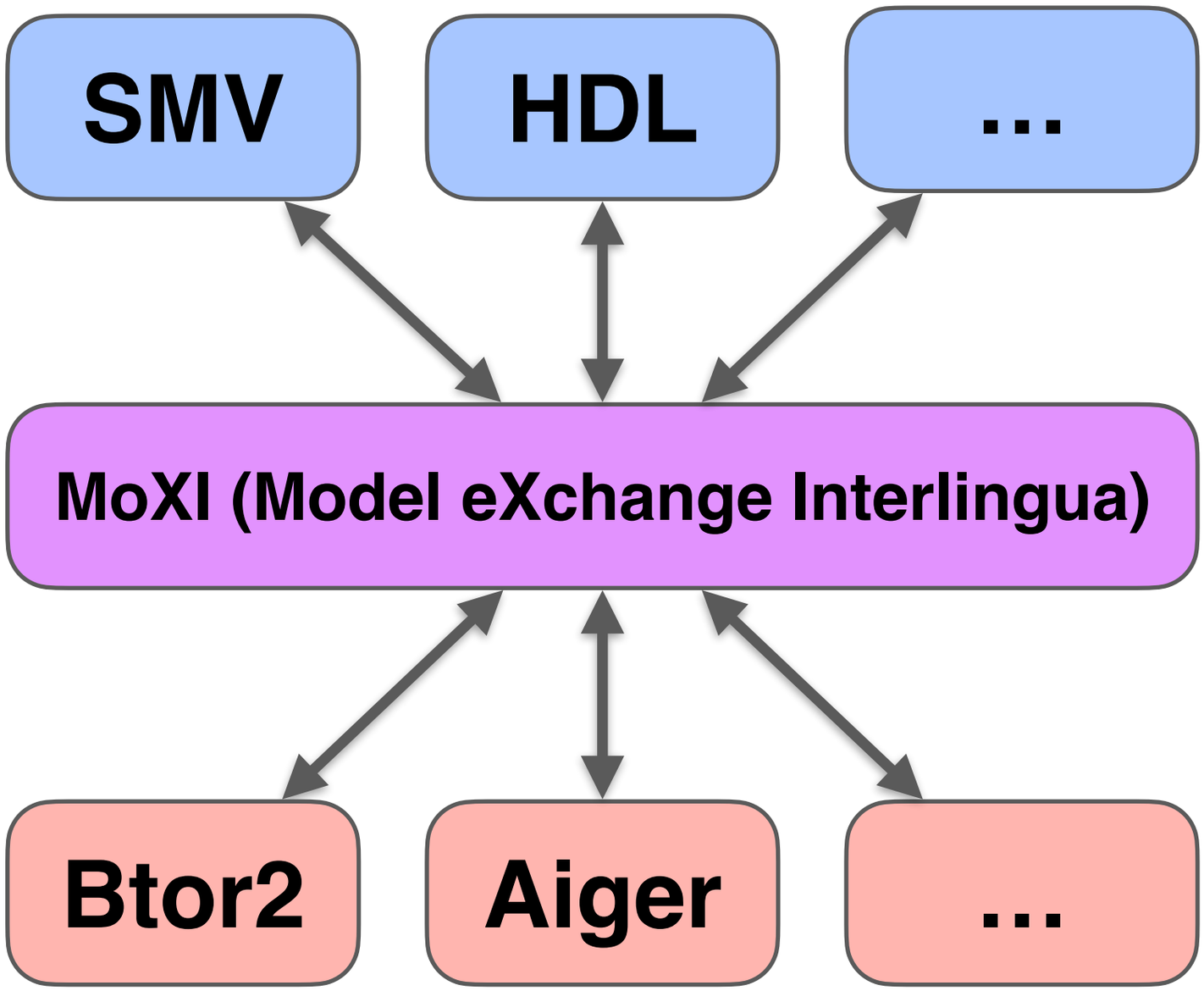




Mary the Model-Checking Researcher

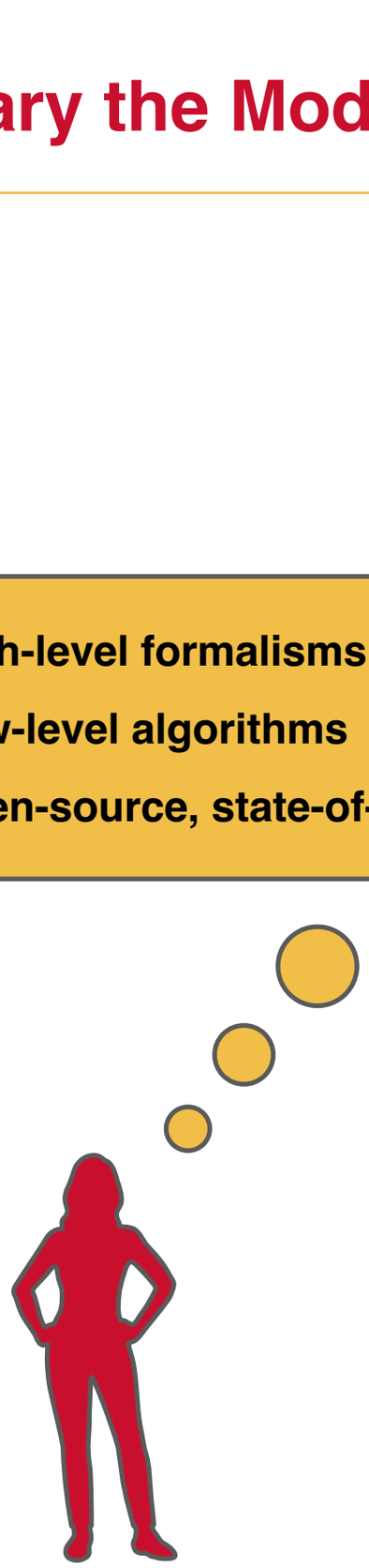
- High-level formalisms
- Low-level algorithms
- Open-source, state-of-the art tools

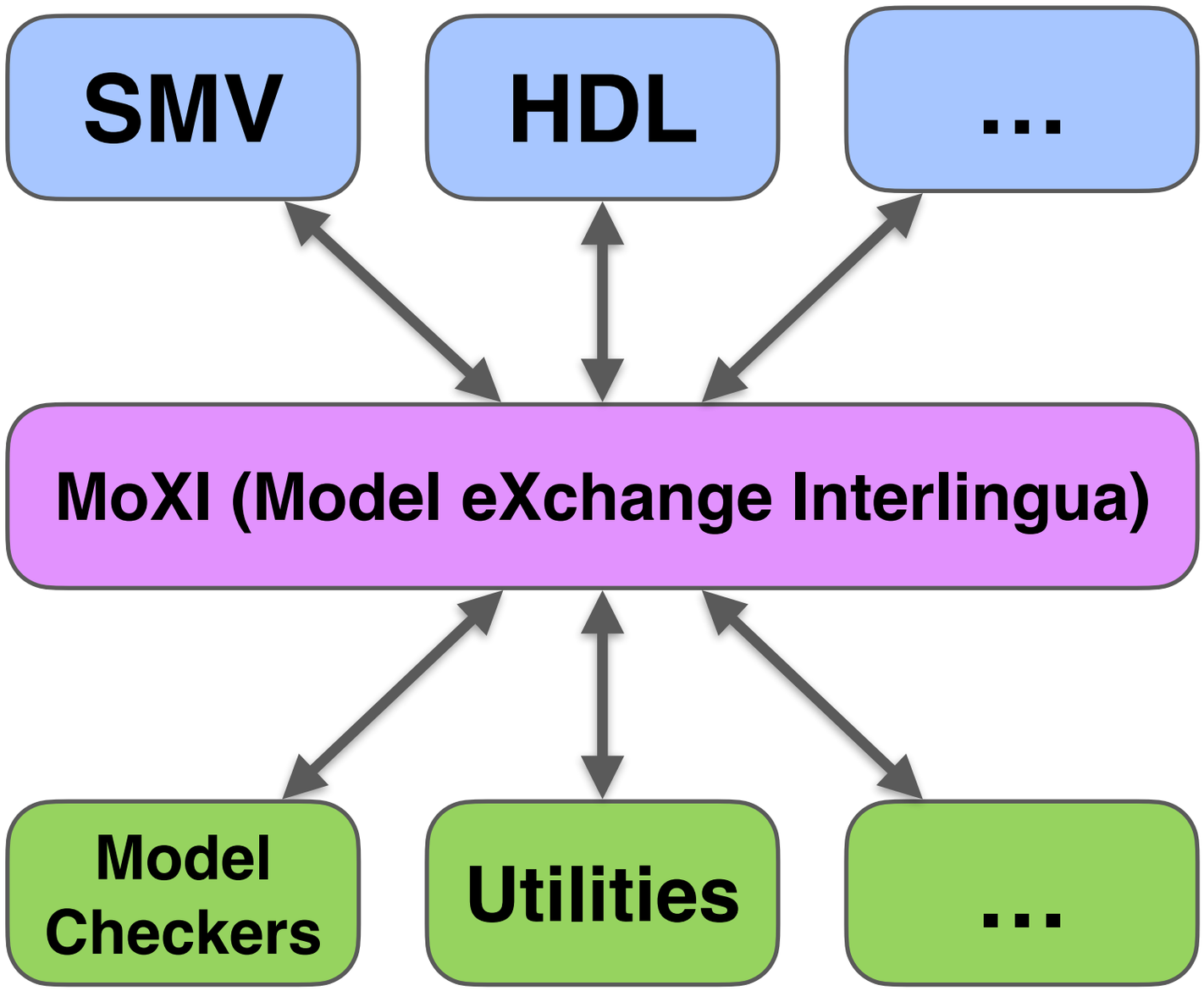




Mary the Model-Checking Researcher

- High-level formalisms
- Low-level algorithms
- Open-source, state-of-the art tools



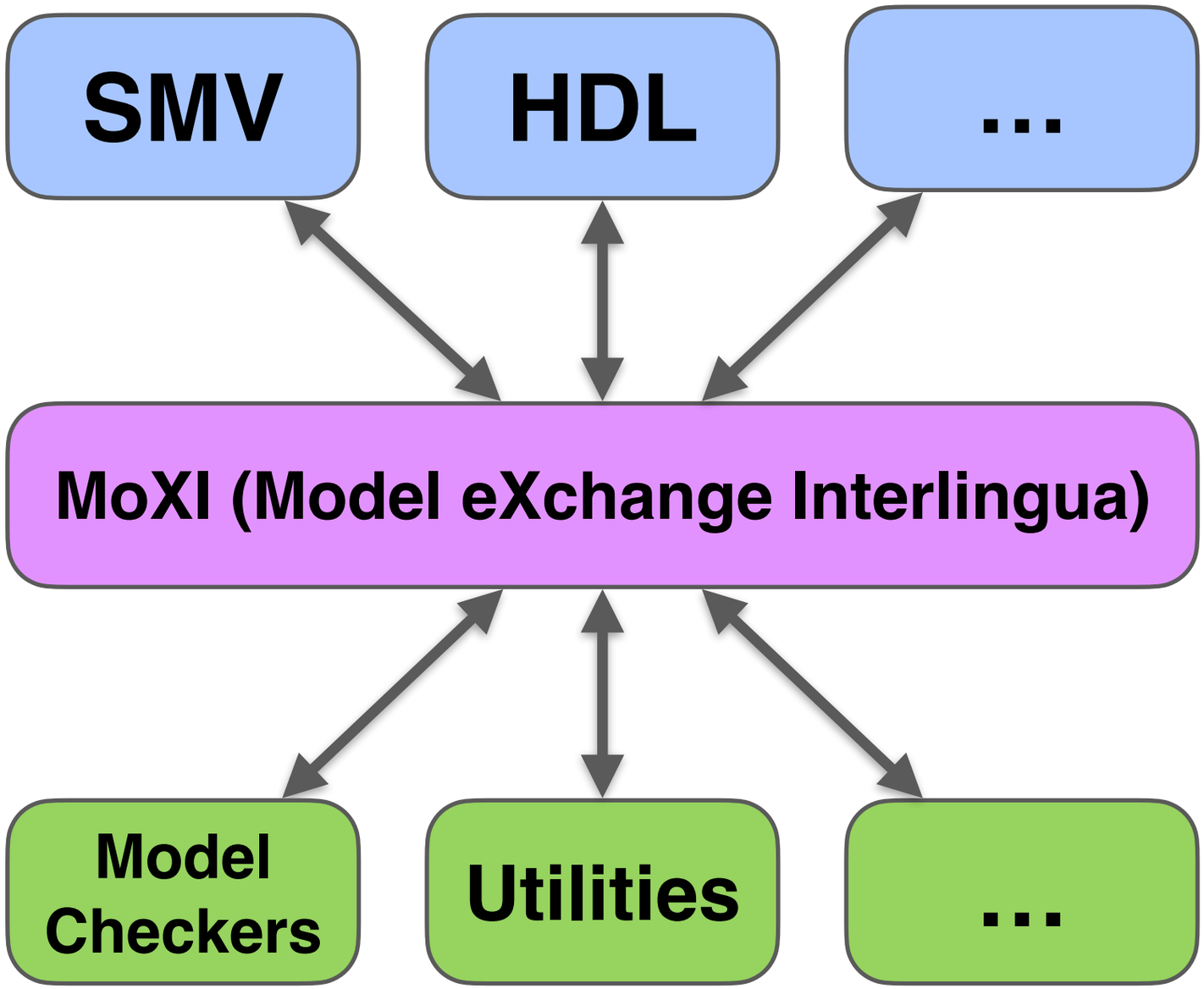


Mary the Model-Checking Researcher

- High-level formalisms
- Low-level algorithms
- Open-source, state-of-the art tools

**MoXIChecker

https://arxiv.org/pdf/2407.15551



MoXI Example

MoXI Example


```
(define-system Delay)
```

MoXI Example


```
(define-system Delay
   :input ((i Int)) :output ((o Int)) :local ((s Int))
)
```

MoXI Example


```
(define-system Delay
   :input ((i Int)) :output ((o Int)) :local ((s Int))
   :init (= o 0)    :trans (= o' s)   :inv (= s i)
)
```

MoXI Example


```
(define-system Delay
   :input ((i Int)) :output ((o Int)) :local ((s Int))
   :init (= o 0)    :trans (= o' s)   :inv (= s i)
   :subsys (S (…))
)
```

MoXI Example


```
(define-system Delay
   :input ((i Int)) :output ((o Int)) :local ((s Int))
   :init (= o 0)    :trans (= o' s)   :inv (= s i)
)

(check-system Delay)
```

MoXI Example


```
(define-system Delay
   :input ((i Int)) :output ((o Int)) :local ((s Int))
   :init (= o 0)    :trans (= o' s)   :inv (= s i)
)

(check-system Delay
   :input ((i Int)) :output ((o Int)) :local ((s Int))
)
```

MoXI Example


```
(define-system Delay
   :input ((i Int)) :output ((o Int)) :local ((s Int))
   :init (= o 0)    :trans (= o' s)   :inv (= s i)
)

(check-system Delay
   :input ((i Int)) :output ((o Int)) :local ((s Int))
   :reachable (r (= o 10))    :query (qry (r))
)
```

MoXI Example

```
(define-system Delay
    :input ((i Int)) :output ((o Int)) :local ((s Int))
    :init (= o 0)    :trans (= o' s)   :inv (= s i)
)
(check-system Delay
    :input ((i Int)) :output ((o Int)) :local ((s Int))
    :reachable (r (= o 10))    :query (qry (r))
)
```

MoXI Example

```
(define-system Delay
    :input ((i Int)) :output ((o Int)) :local ((s Int))
    :init (= o 0)    :trans (= o' s)   :inv (= s i)
)
(check-system Delay
    :input ((i Int)) :output ((o Int)) :local ((s Int))
    :reachable (r (= o 10))    :query (qry (r))
)
```


```
(check-system-response Delay)
```

MoXI Example

```
(define-system Delay
    :input ((i Int)) :output ((o Int)) :local ((s Int))
    :init (= o 0)    :trans (= o' s)   :inv (= s i)
)
(check-system Delay
    :input ((i Int)) :output ((o Int)) :local ((s Int))
    :reachable (r (= o 10))    :query (qry (r))
)
```


```
(check-system-response Delay
   :query (qry :result sat :trace t)
)
```

MoXI Example

```
(define-system Delay
    :input ((i Int)) :output ((o Int)) :local ((s Int))
    :init (= o 0)    :trans (= o' s)   :inv (= s i)
)
(check-system Delay
    :input ((i Int)) :output ((o Int)) :local ((s Int))
    :reachable (r (= o 10))    :query (qry (r))
)
```

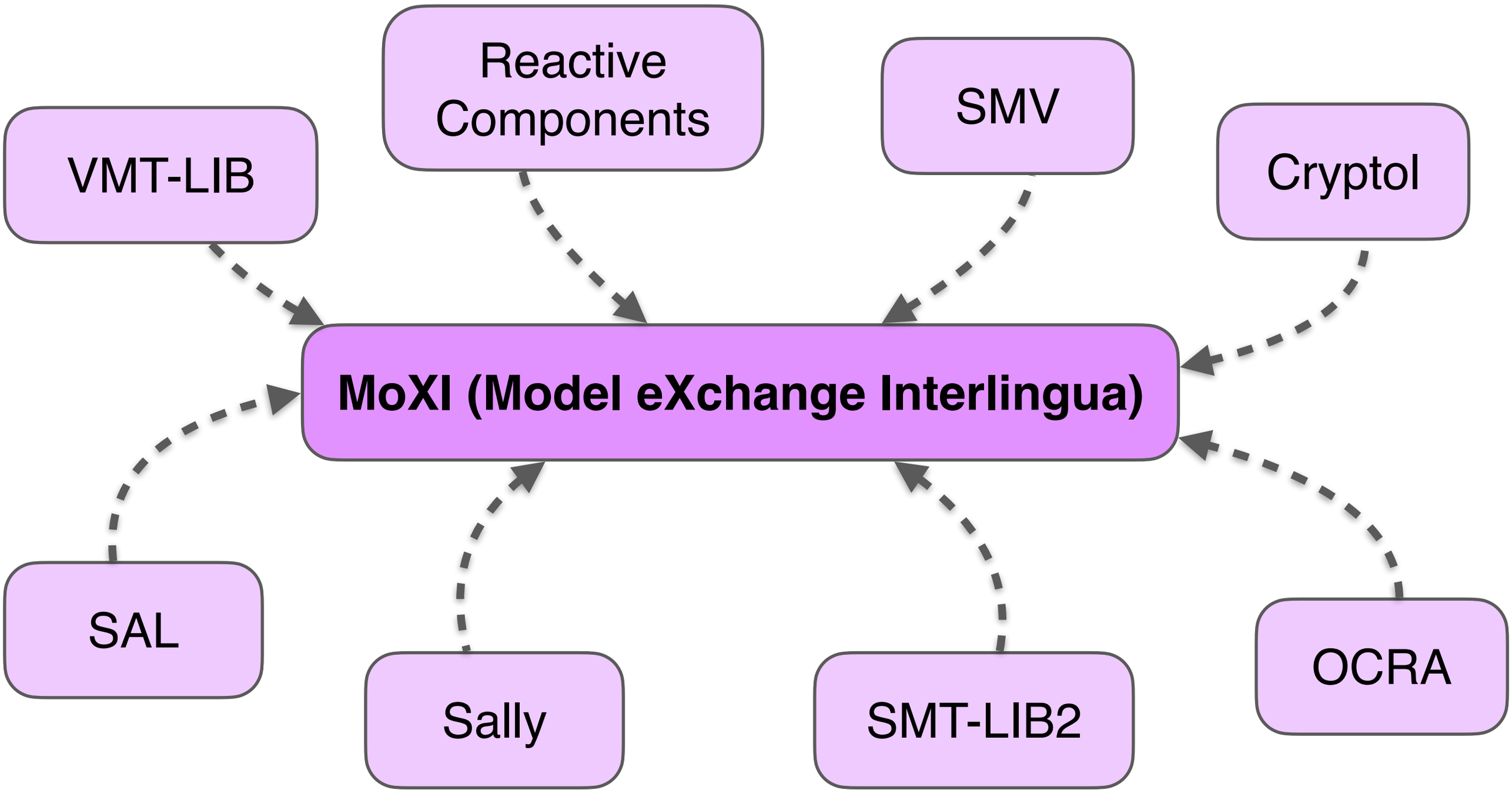

```
(check-system-response Delay
   :query (qry :result sat :trace t)
   :trace (t :prefix p)
)
```

MoXI Example

```
(define-system Delay
    :input ((i Int)) :output ((o Int)) :local ((s Int))
    :init (= o 0)    :trans (= o' s)   :inv (= s i)
)
(check-system Delay
    :input ((i Int)) :output ((o Int)) :local ((s Int))
    :reachable (r (= o 10))    :query (qry (r))
)
```

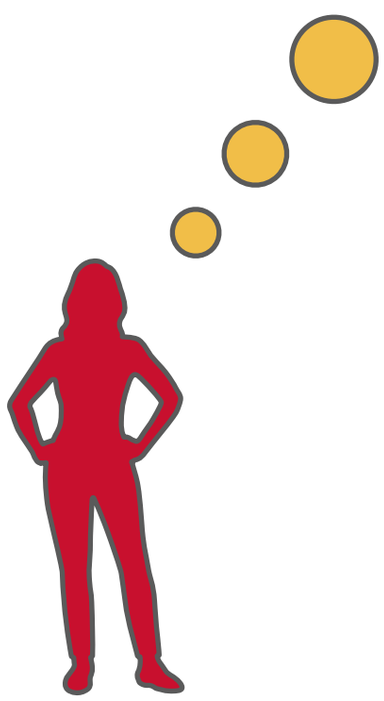

```
(check-system-response Delay
   :query (qry :result sat :trace t)
   :trace (t :prefix p)
   :trail (p ( (0 (i 10) (o  0) (s 10))
               (1 (i  0) (o 10) (s  0))))
)
```

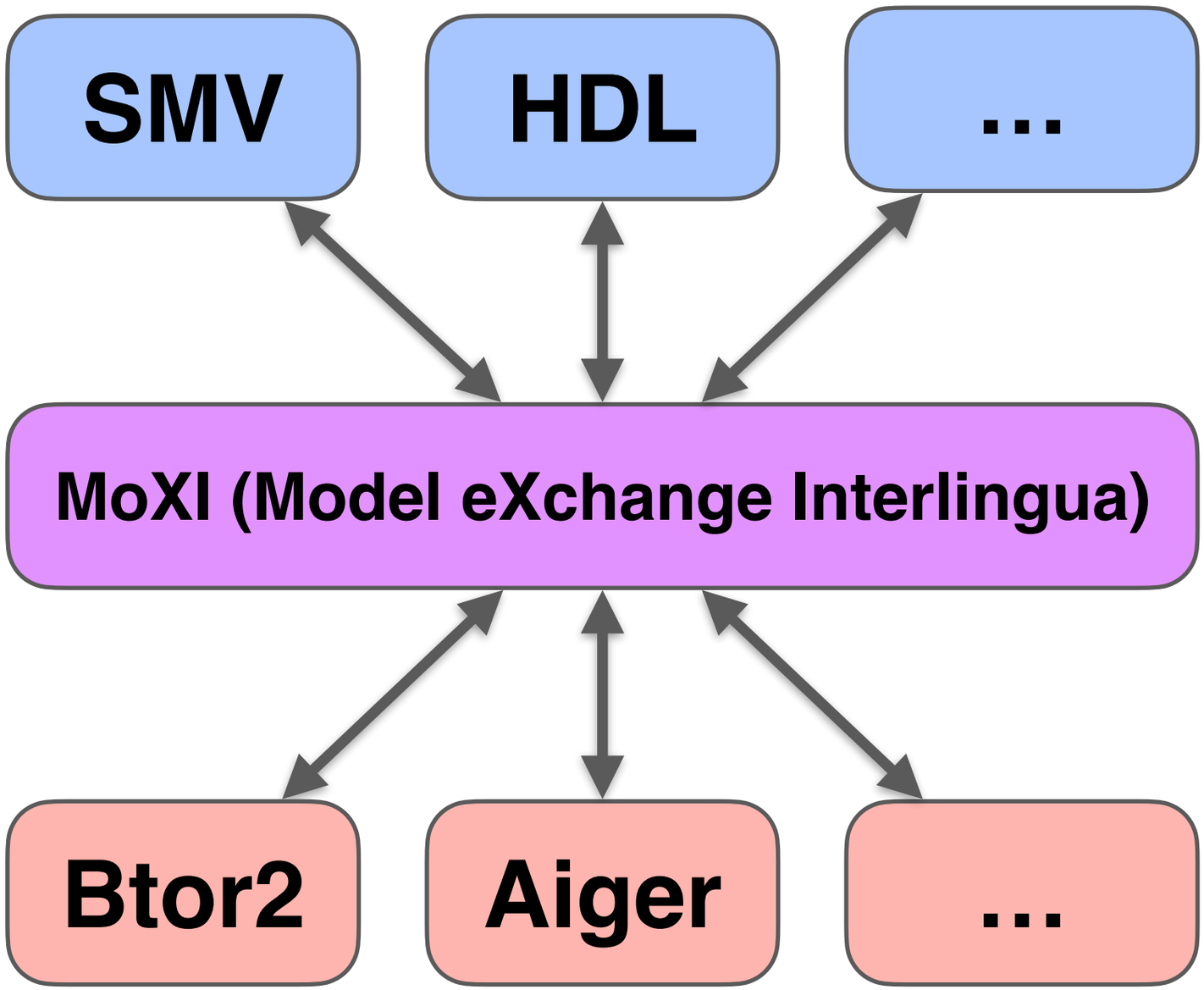
MoXI Influences



Mary the Model-Checking Researcher

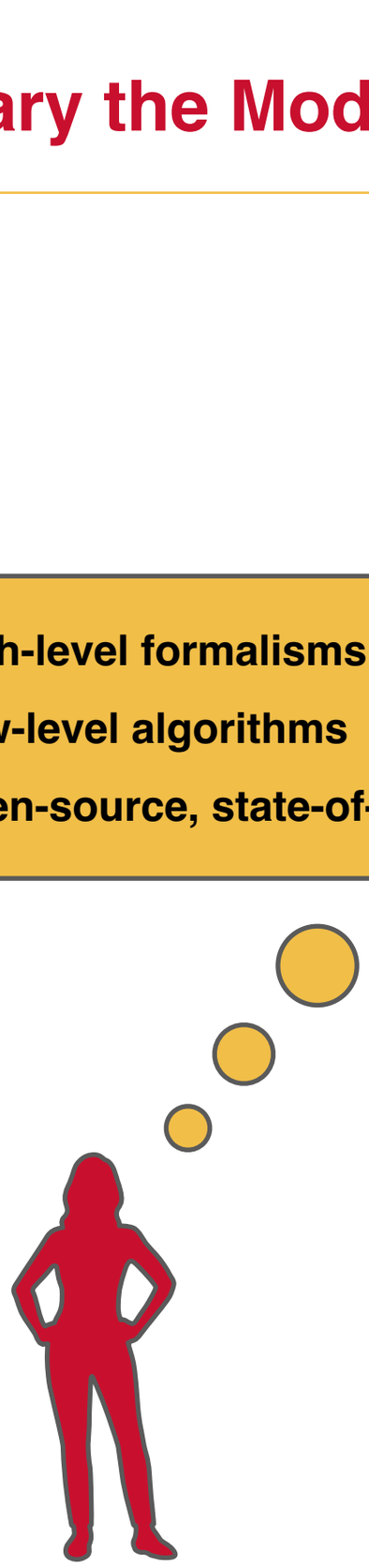
- High-level formalisms
- Low-level algorithms
- Open-source, state-of-the art tools

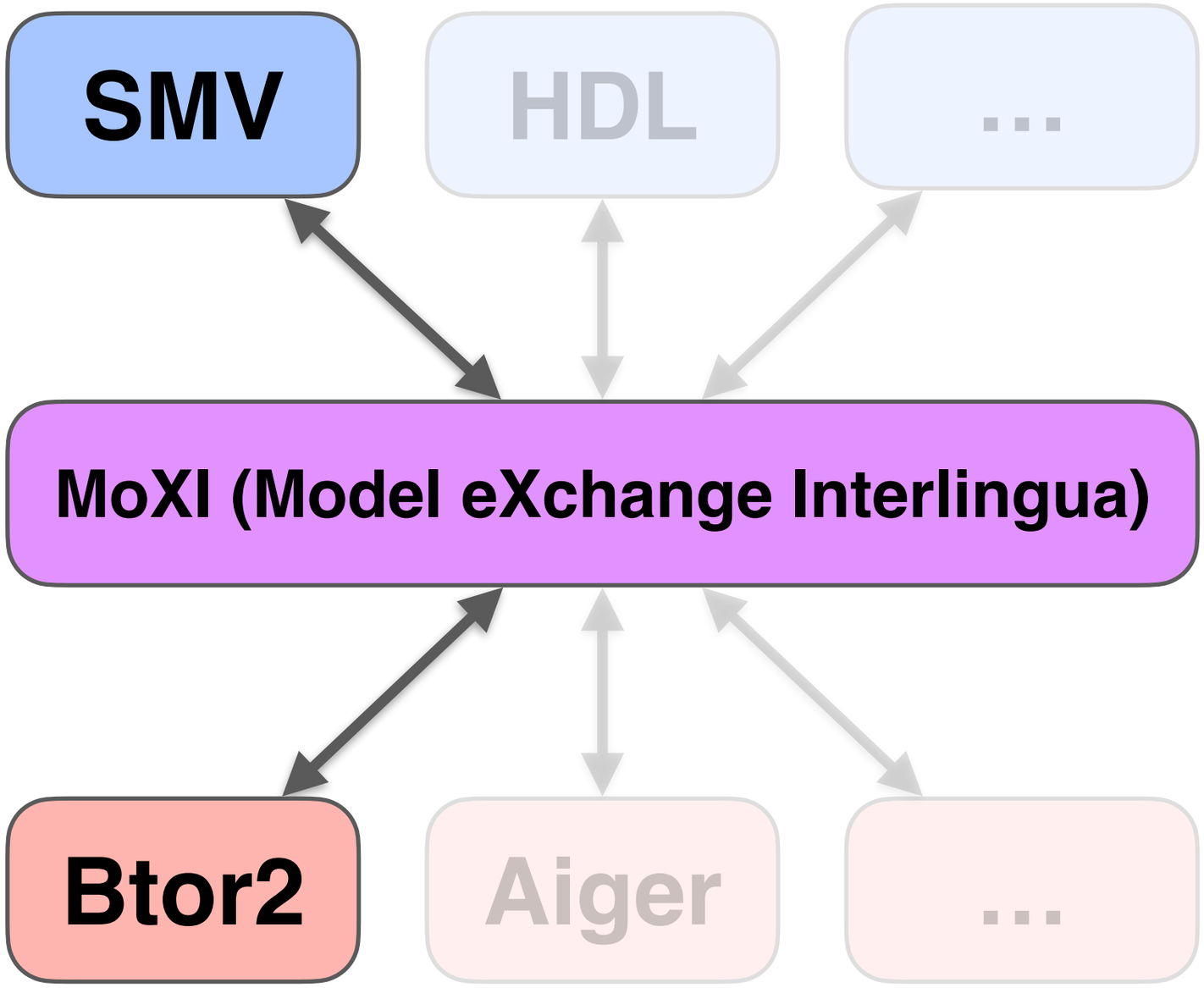




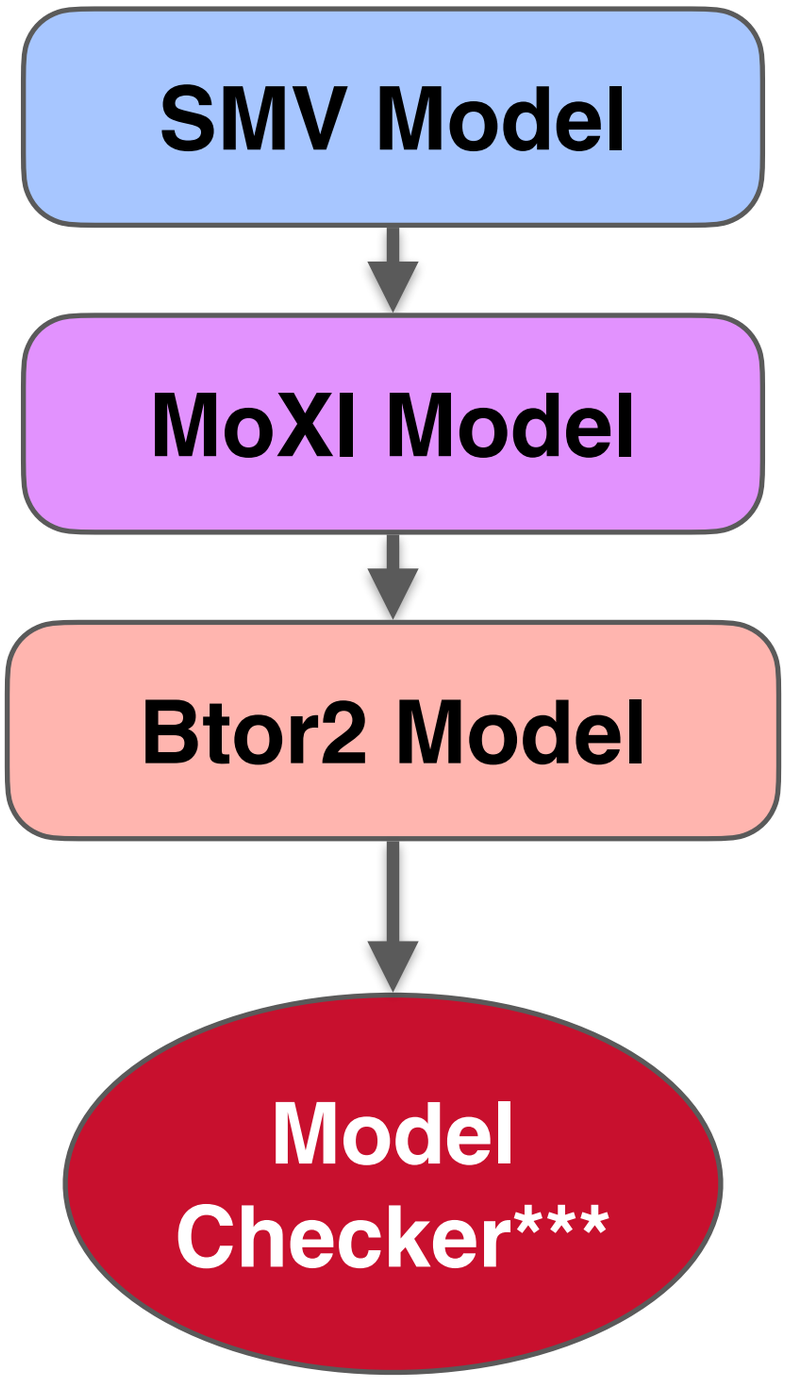
Mary the Model-Checking Researcher

- High-level formalisms
- Low-level algorithms
- Open-source, state-of-the art tools



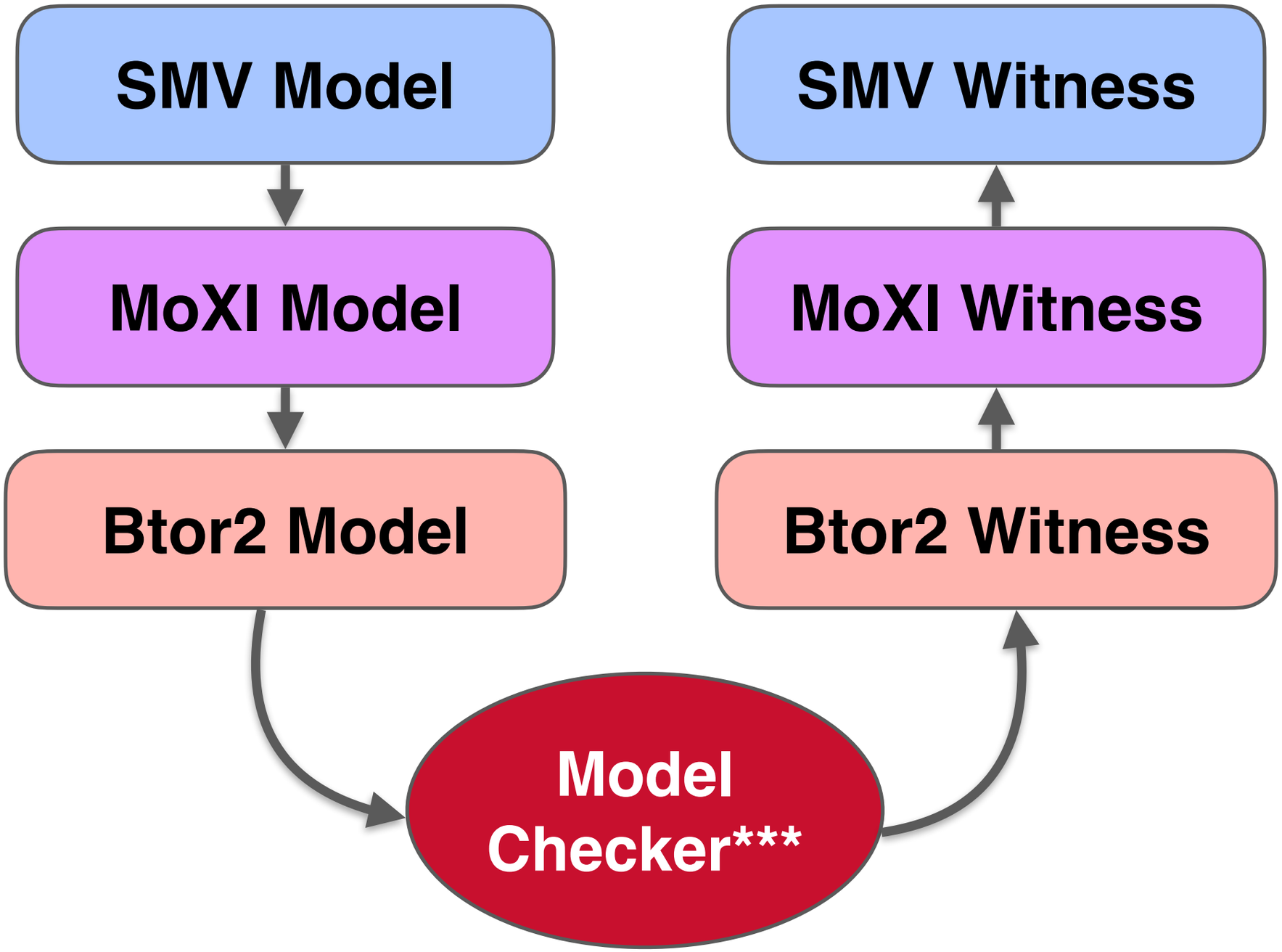


Model-Checking Flow



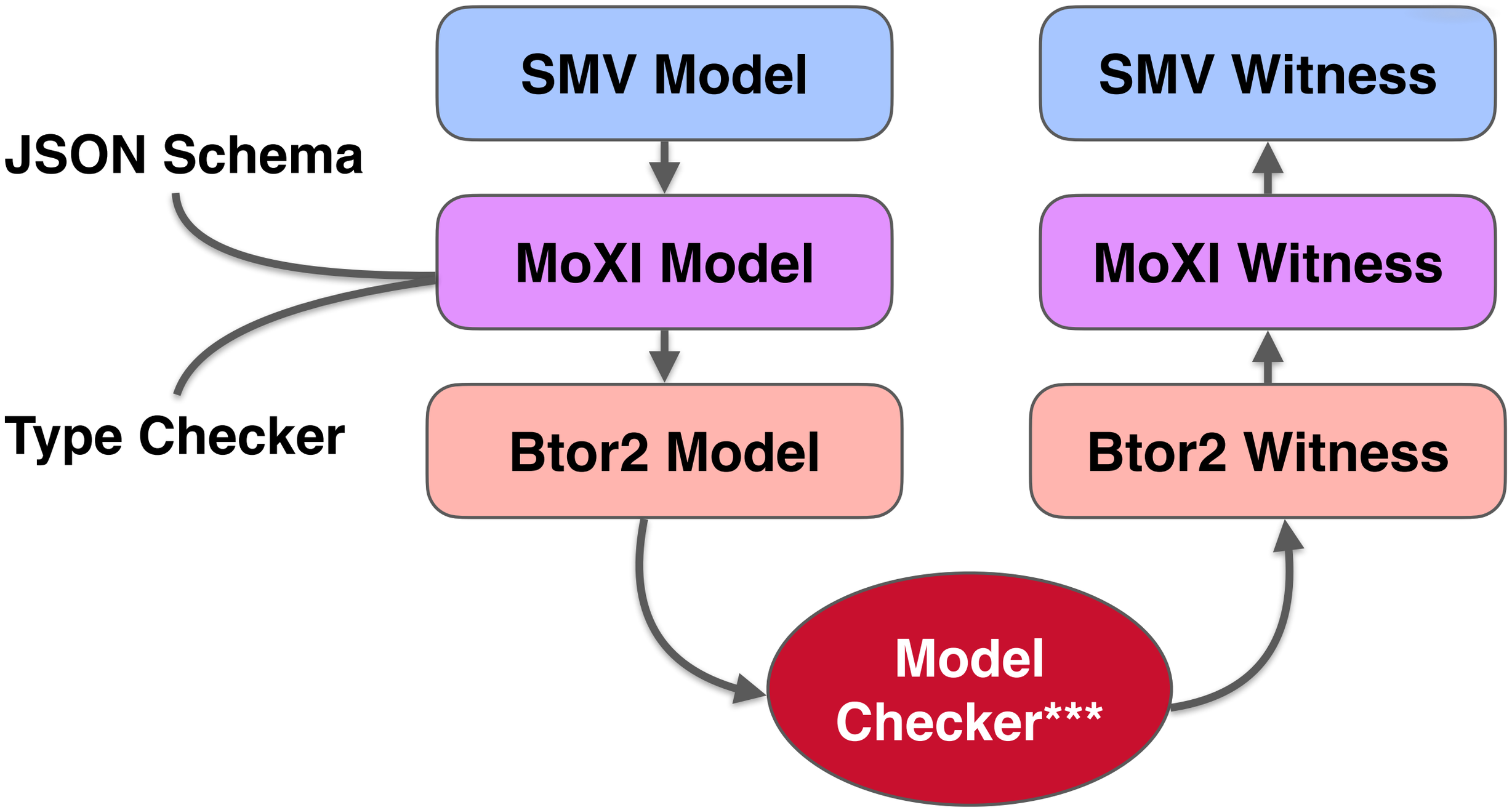
***AVR/Pono/BtorMC

Model-Checking Flow



***AVR/Pono/BtorMC

Model-Checking Flow



***AVR/Pono/BtorMC

Model-Checking Flow

Benchmarks

SMV Model

MoXI Model

Btor2 Model

Model Checker***

Btor2 Witness

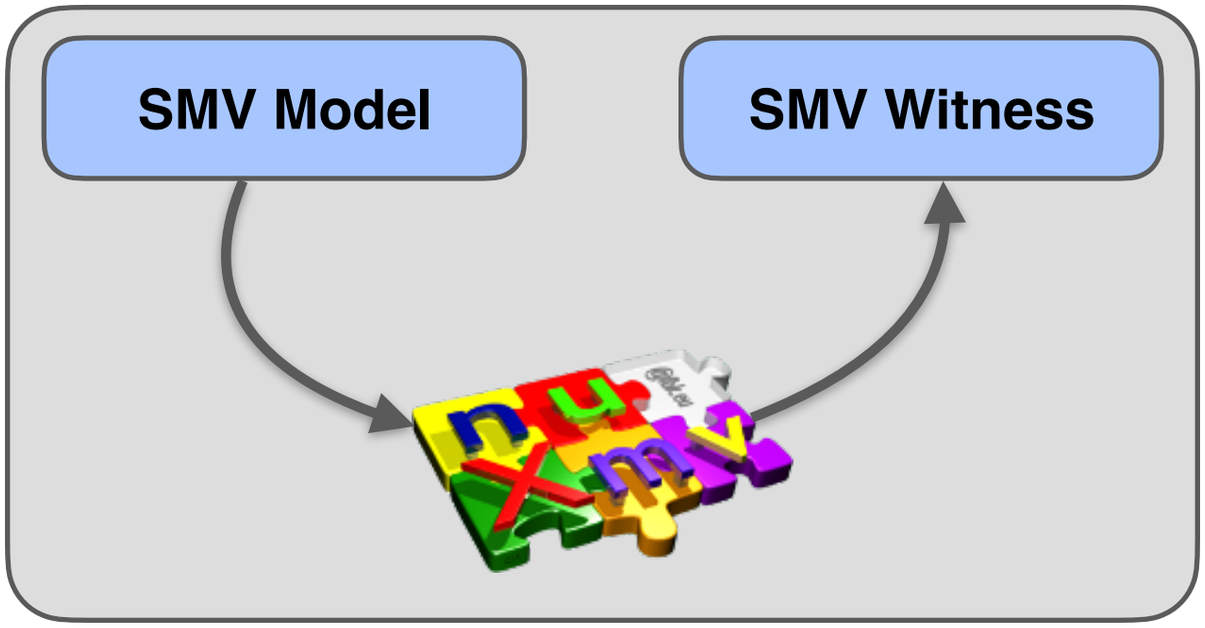
MoXI Witness

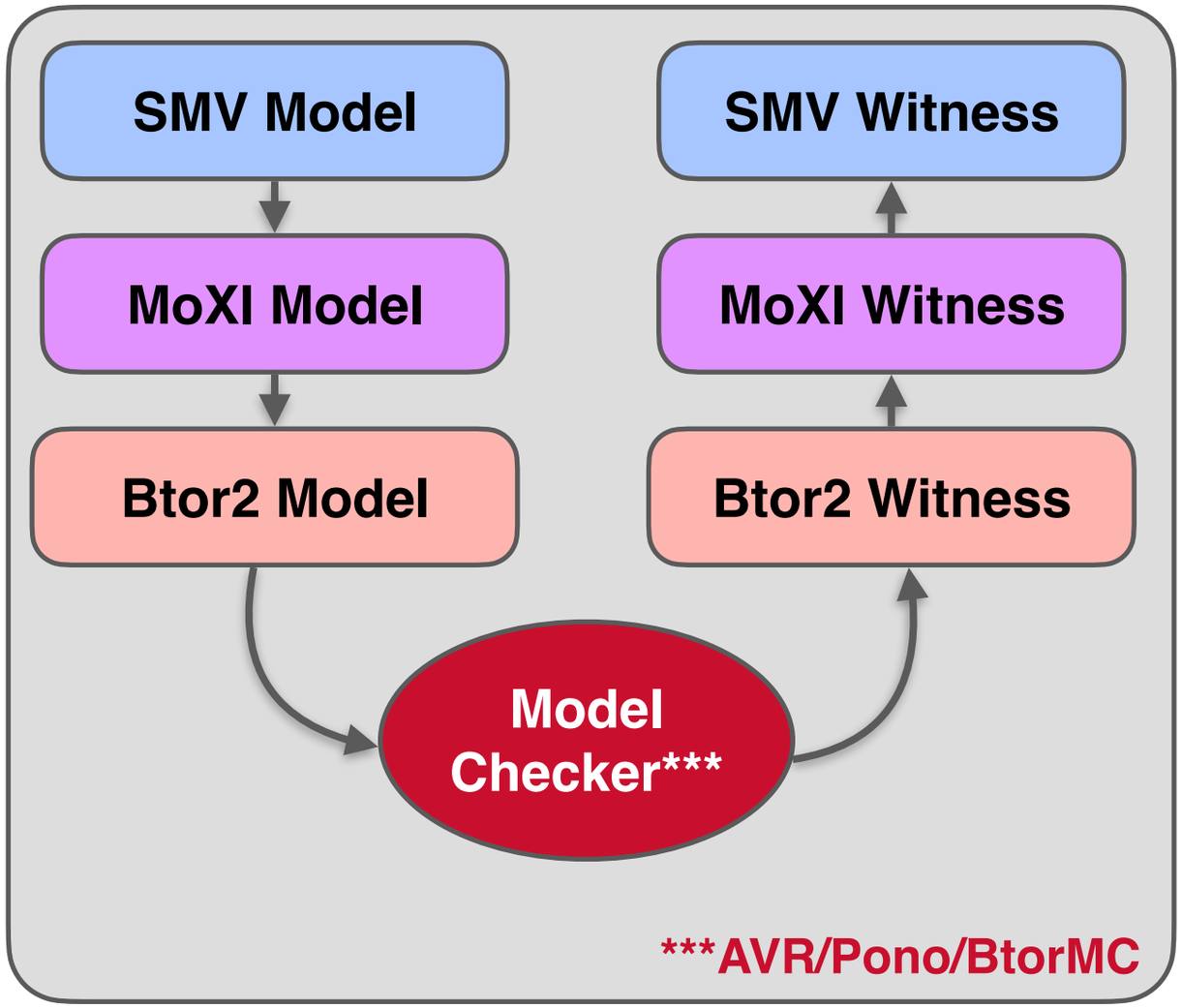
SMV Witness

MoXI Benchmarks

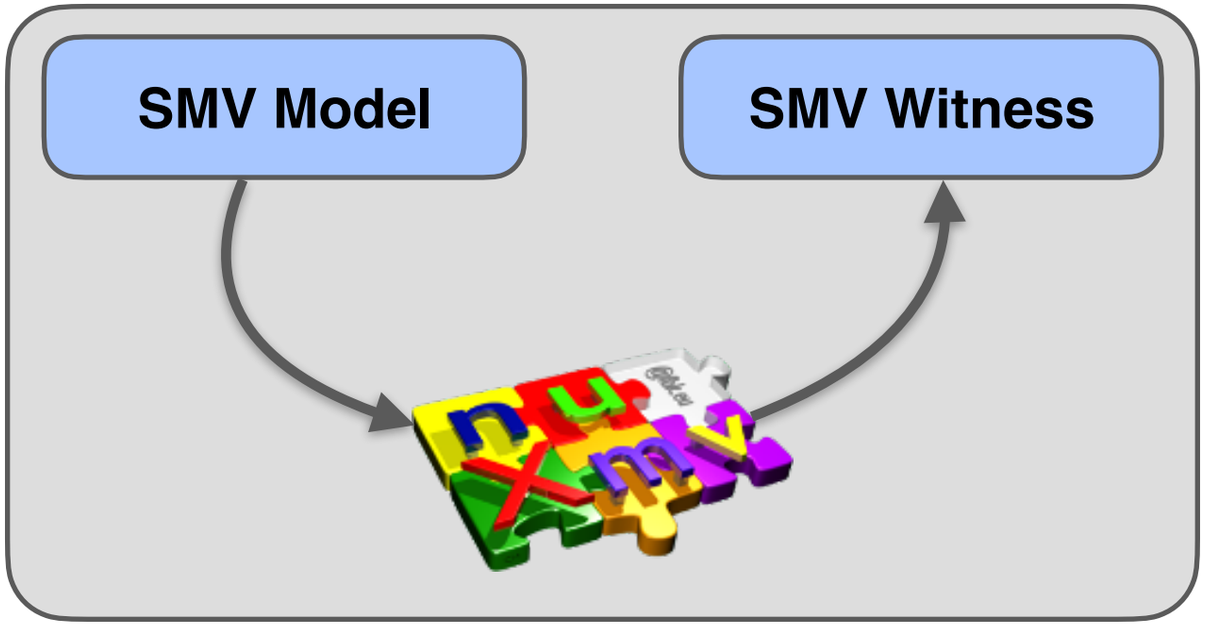
***AVR/Pono/BtorMC

Experimental Evaluation

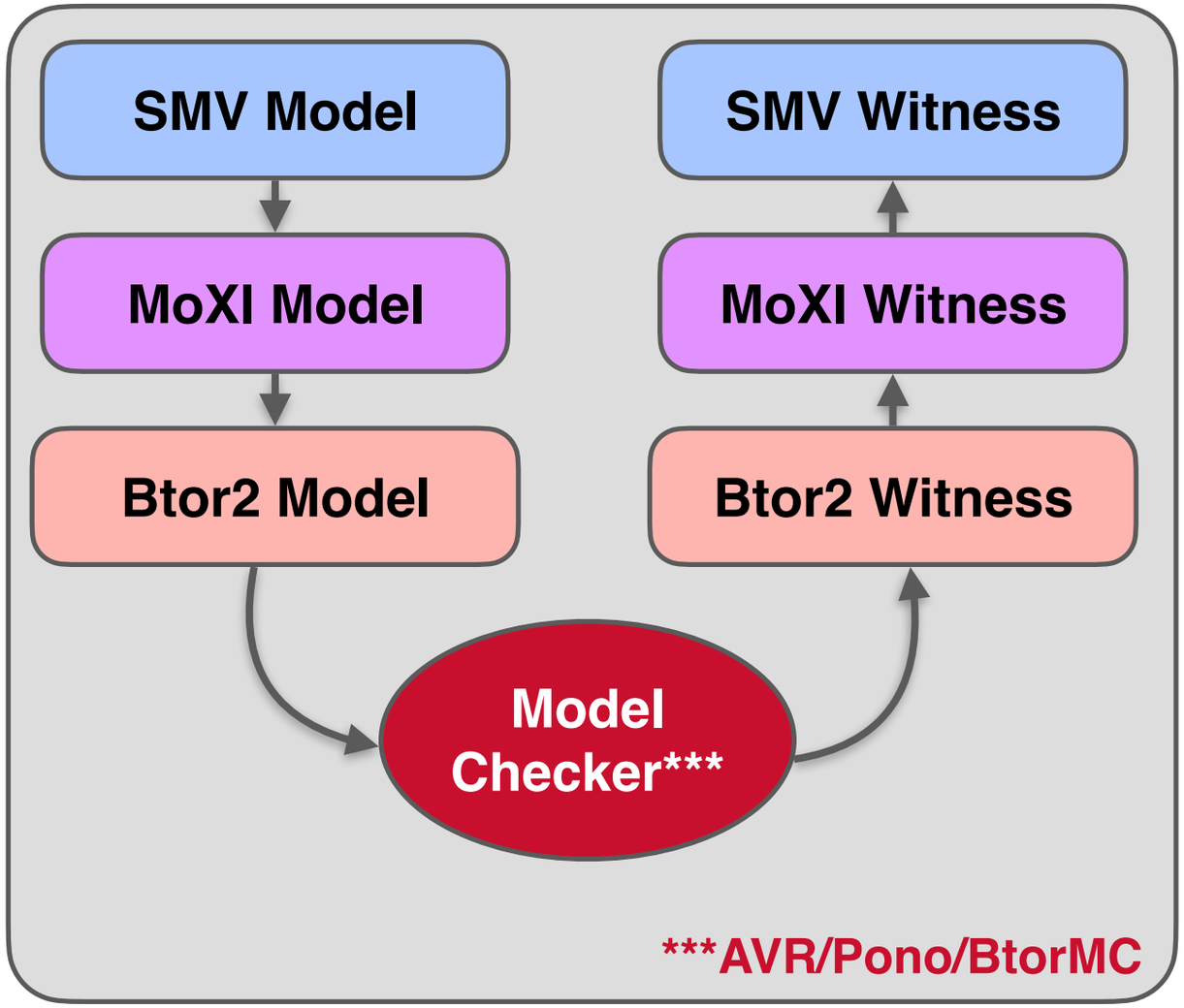




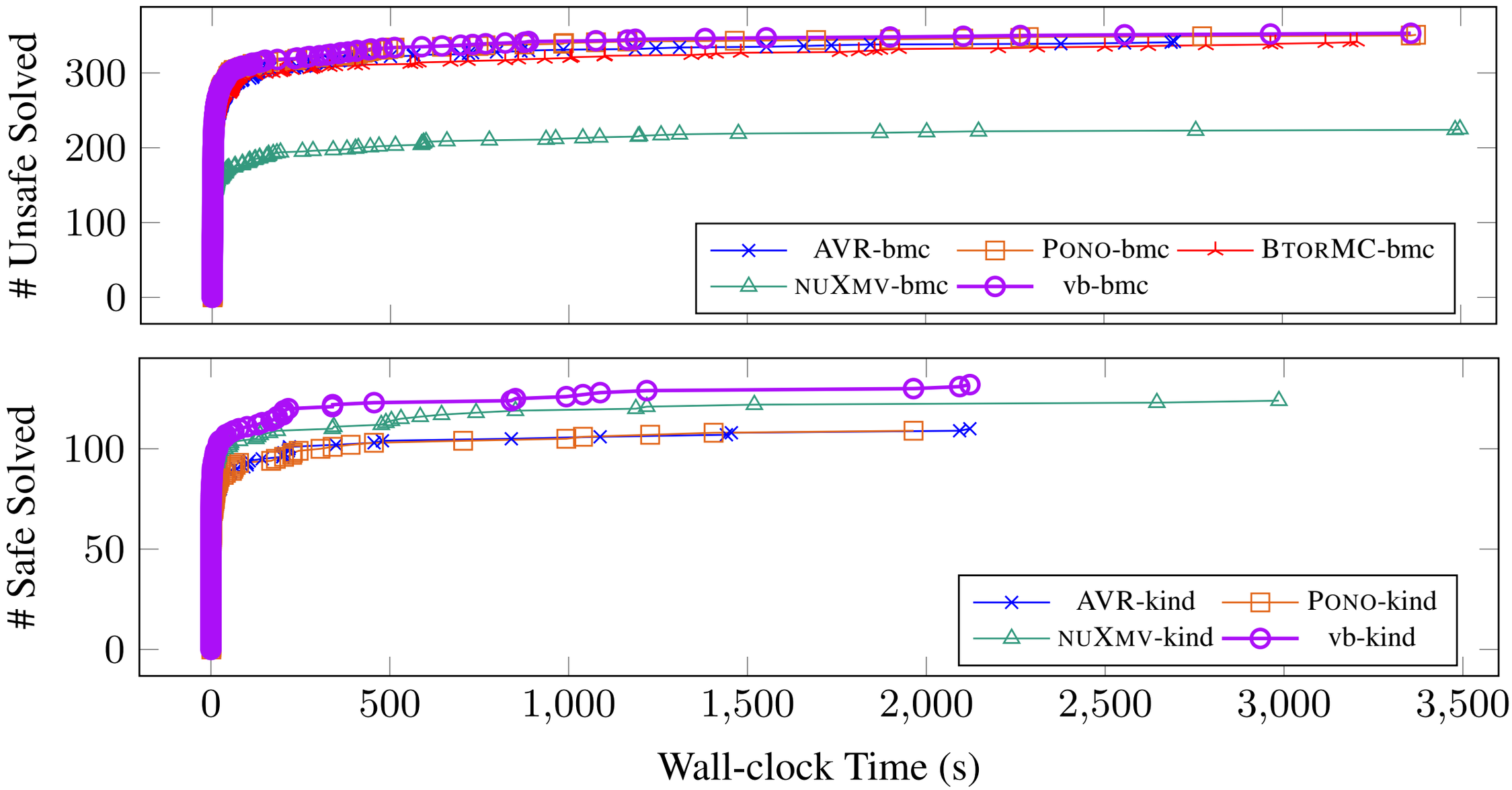
Experimental Evaluation



- BMC
- K-induction



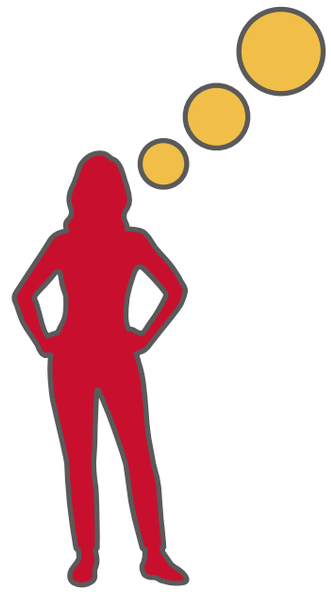
Experimental Evaluation



Conclusion

- New **platform** for model-checking research
- Implemented prototype **translation model-checking flow**
- Includes **translators, type checker, JSON schema, benchmark set**

- ✓ **High-level formalisms**
- ✓ **Low-level algorithms**
- ✓ **Open-source, state-of-the art tools**



Website

modelchecker.github.io

Acknowledgements

- NSF for funding this work
- Technical advisory board for invaluable feedback

GitHub

github.com/ModelChecker/moxi-mc-flow