ModelPlex: Verified Runtime Validation of Verified CPS Models

From Model Checking to Checking Models

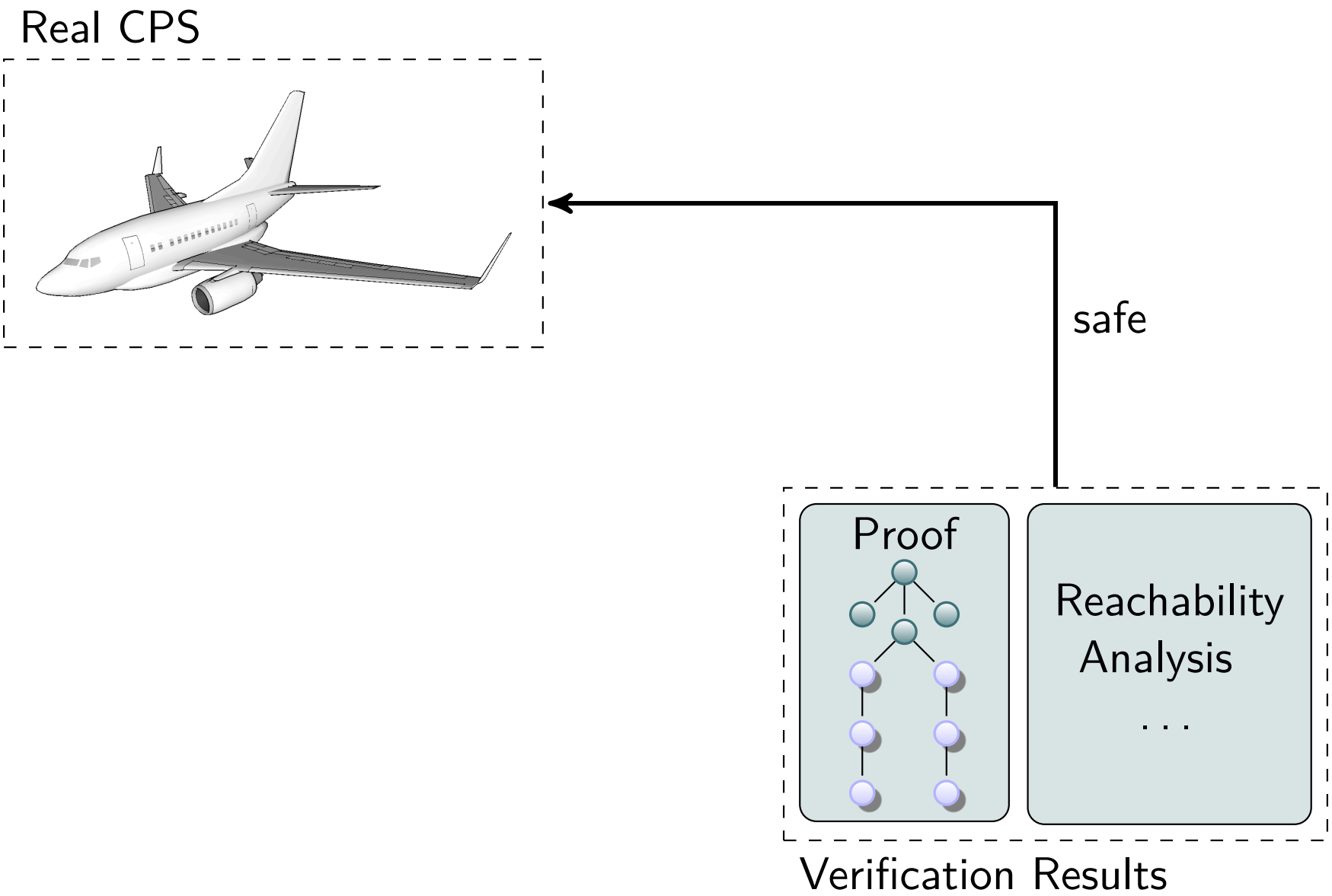
Stefan Mitsch André Platzer

Computer Science Department, Carnegie Mellon University

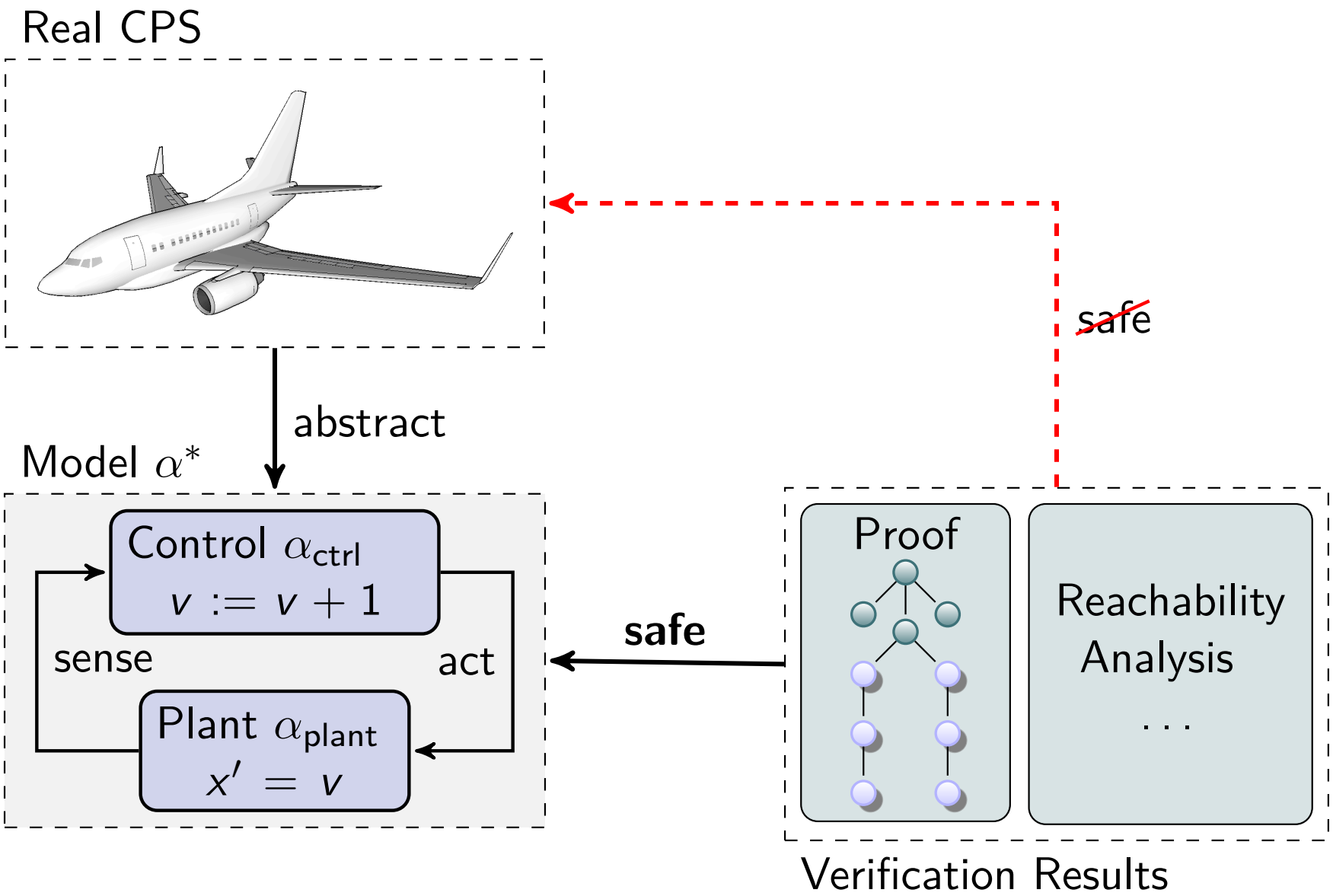
Clarke Symposium, Sept. 20, 2014

For details, see ModelPlex paper at RV'14

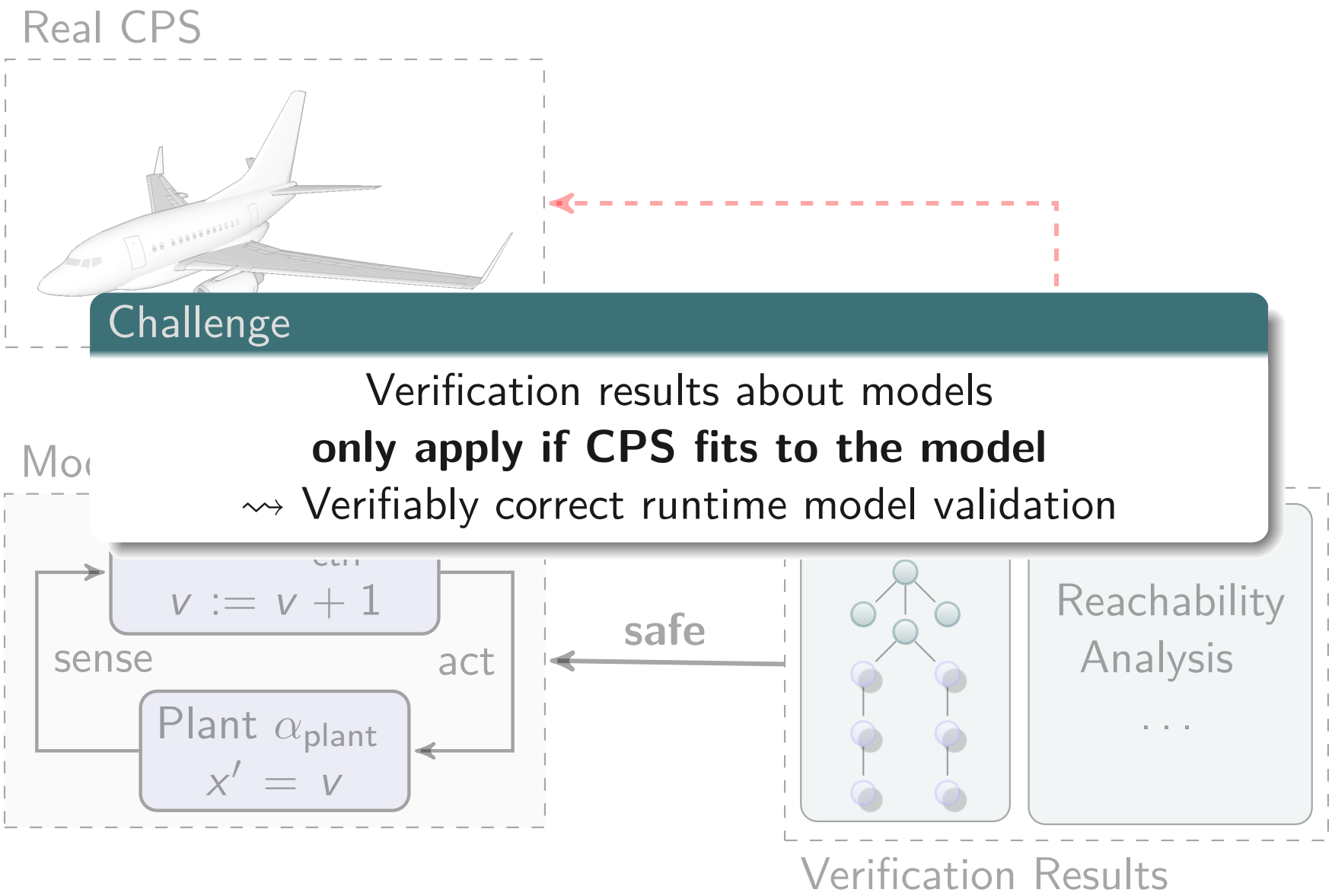
Formal Verification in CPS Development



Formal Verification in CPS Development

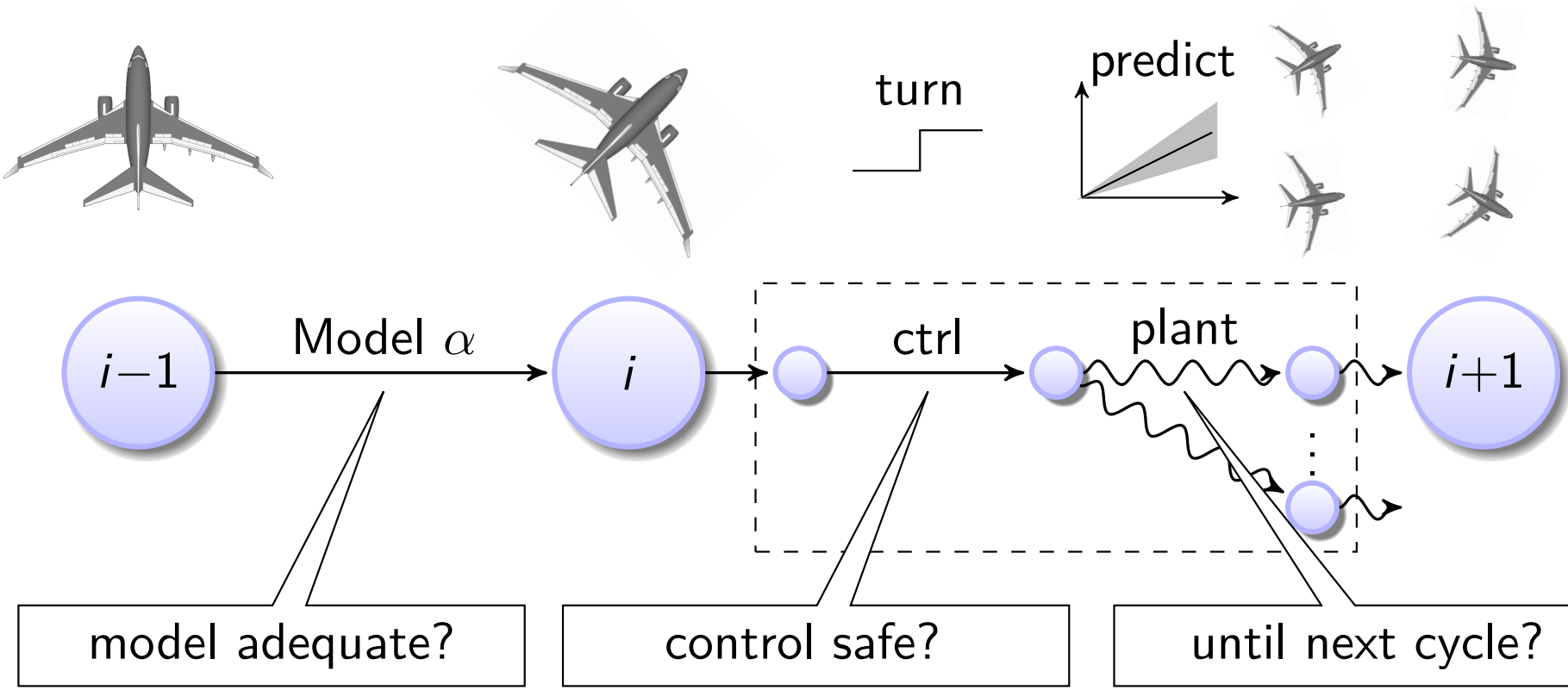


Formal Verification in CPS Development



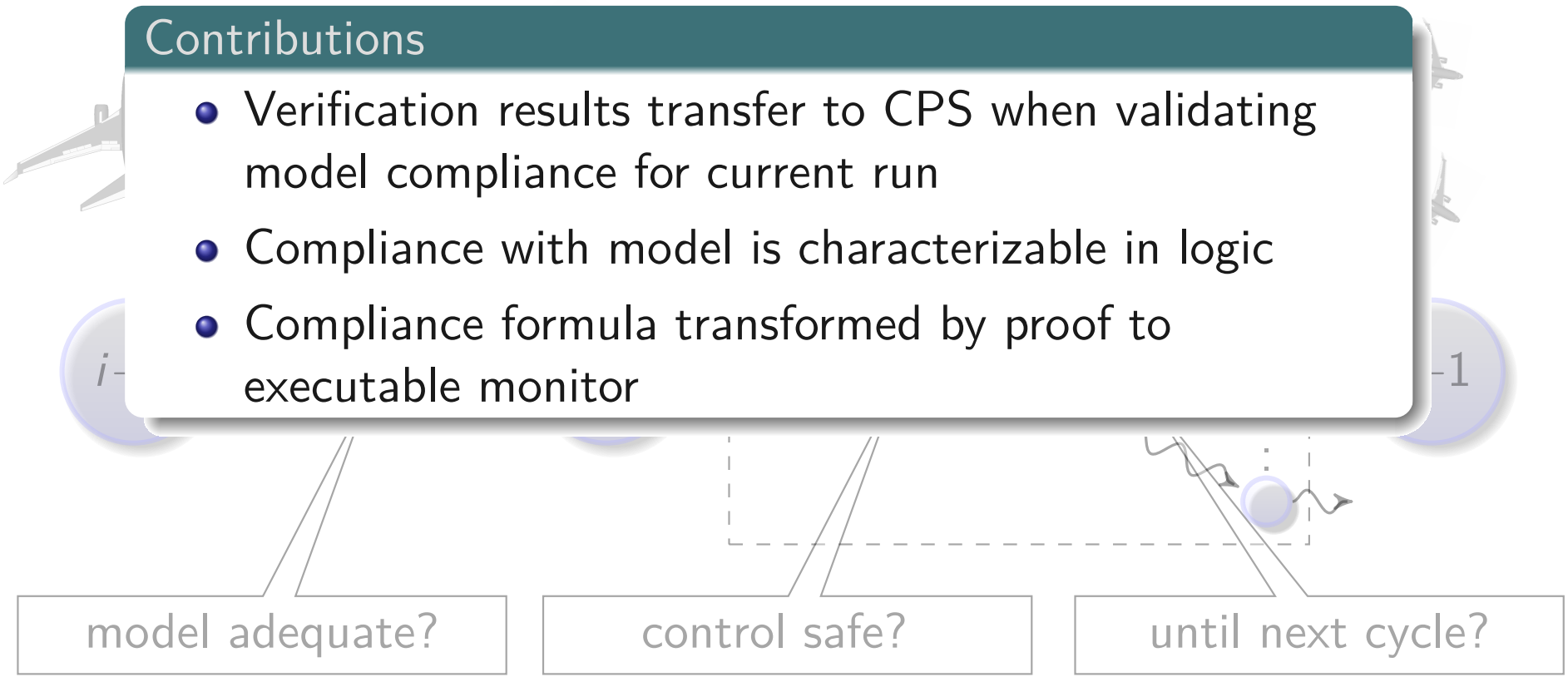
ModelPlex Runtime Model Validation

ModelPlex **ensures that verification results** about models **apply to CPS** implementations



ModelPlex Runtime Model Validation

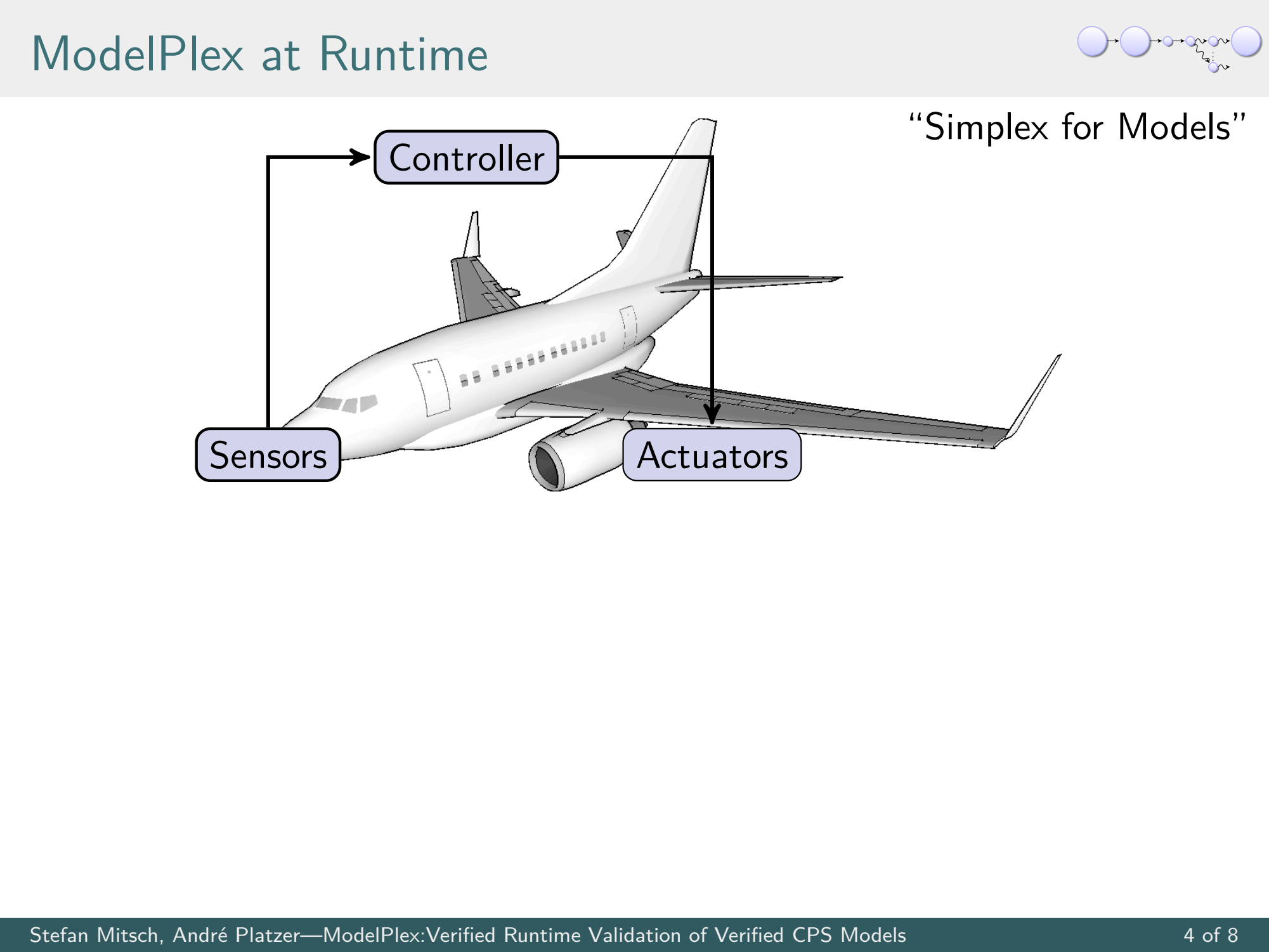
ModelPlex **ensures that verification results** about models **apply to CPS** implementations



Contributions

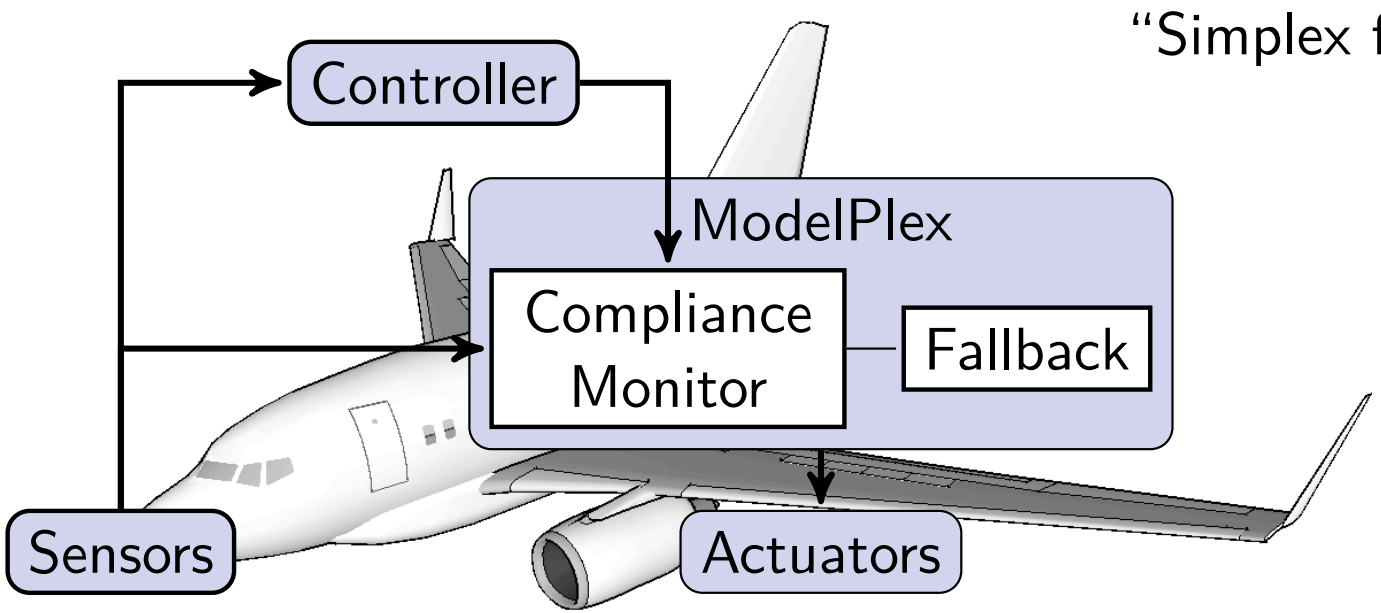
- Verification results transfer to CPS when validating model compliance for current run
- Compliance with model is characterizable in logic
- Compliance formula transformed by proof to executable monitor

ModelPlex at Runtime



"Simplex for Models"

ModelPlex at Runtime



Compliance Monitor Checks CPS for compliance with model at runtime

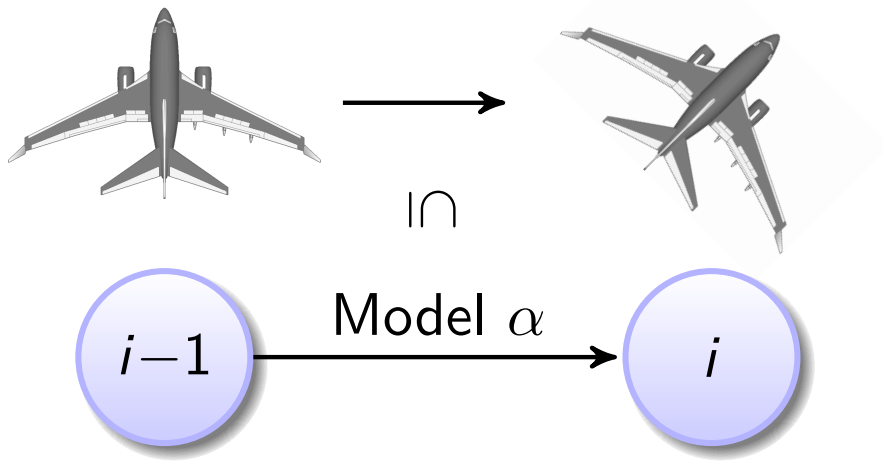
- Model Monitor: model adequate?
- Controller Monitor: control safe?
- Prediction Monitor: until next cycle?

Fallback Safe action, executed when monitor is not satisfied

Challenge What conditions do the monitors need to check to be safe?

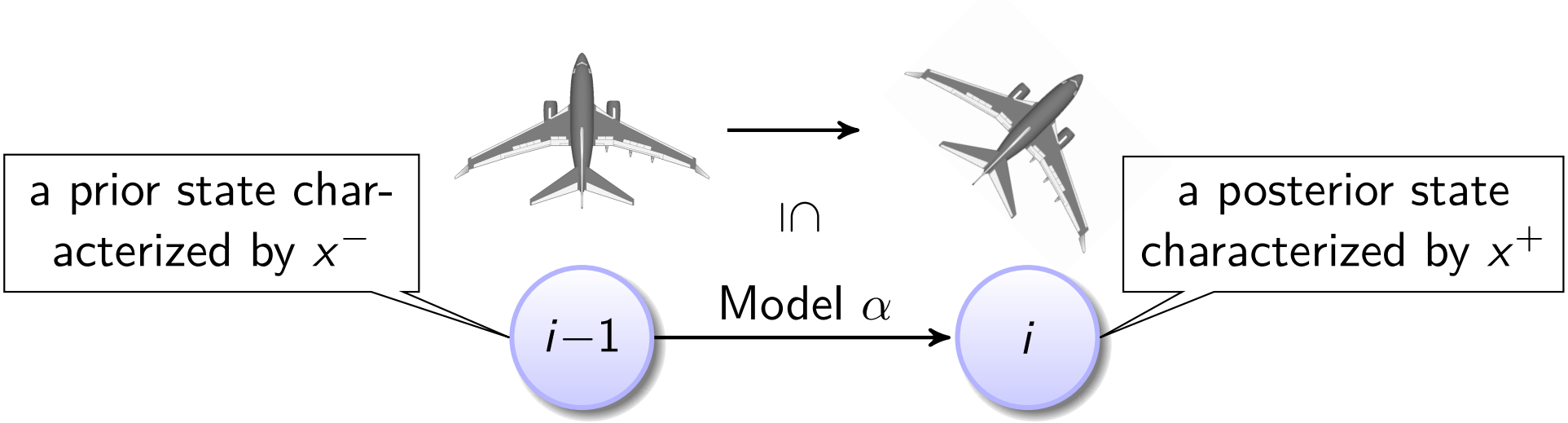
Monitor Characterization

When are two states linked through a run of model α?



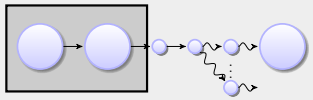
Monitor Characterization

When are two states linked through a run of model α?

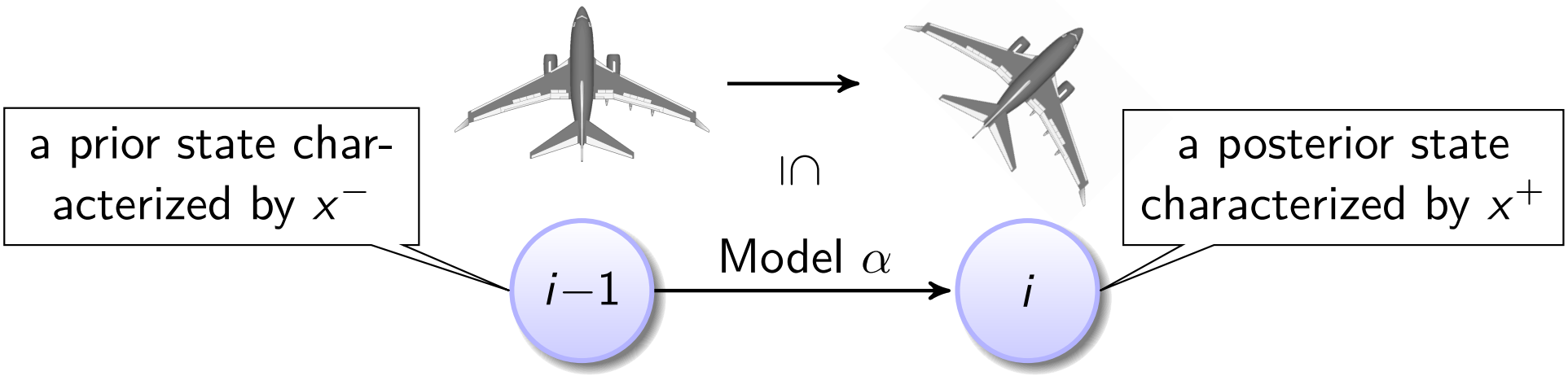


Semantical: $(x^-, x^+) \in \rho(\alpha)$ < reachability relation of α

Monitor Characterization



When are two states linked through a run of model α?



Offline

Semantical: $(x^-, x^+) \in \rho(\alpha)$

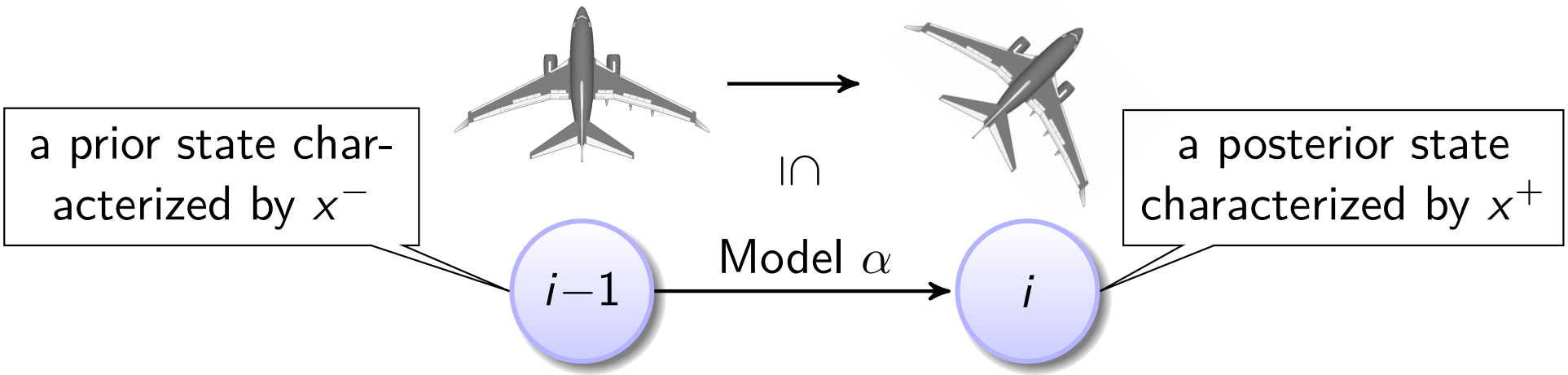
$\Updownarrow$ Theorem

Logic (d$\mathcal{L}$): $(x = x^-) \rightarrow \langle \alpha_{(x)} \rangle (x = x^+)$

starting at $x = x^-$ exists a run of α to a state where $x = x^+$

Monitor Characterization

When are two states linked through a run of model α?



Offline

Semantical: $(x^-, x^+) \in \rho(\alpha)$

$\Updownarrow$ Theorem

Logic (d$\mathcal{L}$): $(x = x^-) \rightarrow \langle \alpha_{(x)} \rangle (x = x^+)$

starting at $x = x^-$ exists a run of α to a state where $x = x^+$

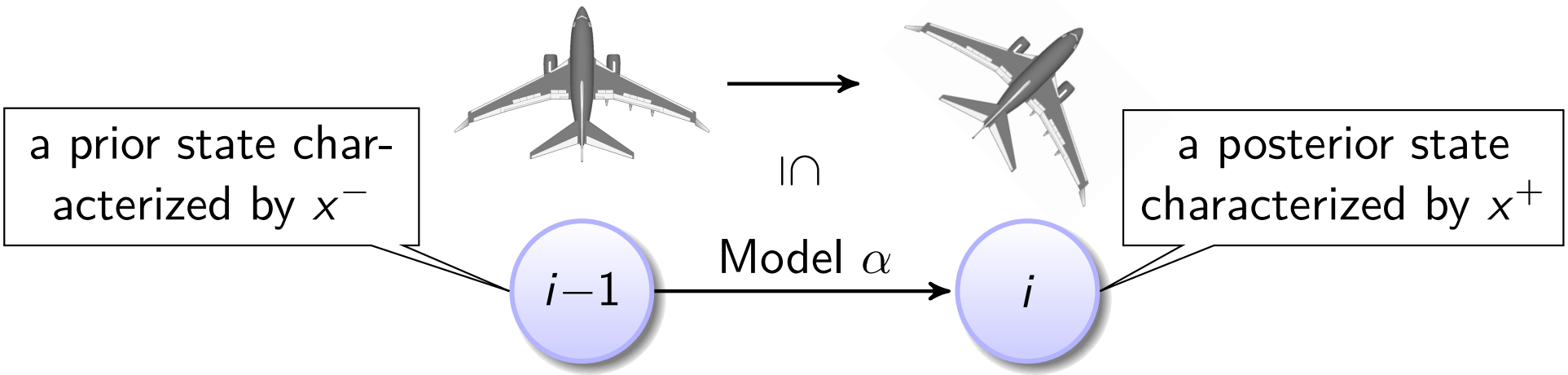
$\Updownarrow$ d$\mathcal{L}$ proof

Real arithmetic: $F(x^-, x^+)$

check at runtime (efficient)

Monitor Characterization

When are two states linked through a run of model α?



Offline

Semantical: $(x^-, x^+) \in \rho(\alpha)$

$\Updownarrow$ Theorem

Logic (d$\mathcal{L}$): $(x = x^-) \rightarrow \langle \alpha_{(x)} \rangle (x = x^+)$

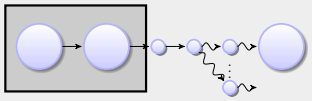
starting at $x = x^-$ exists a run of α to a state where $x = x^+$

$\Uparrow$ d$\mathcal{L}$ proof

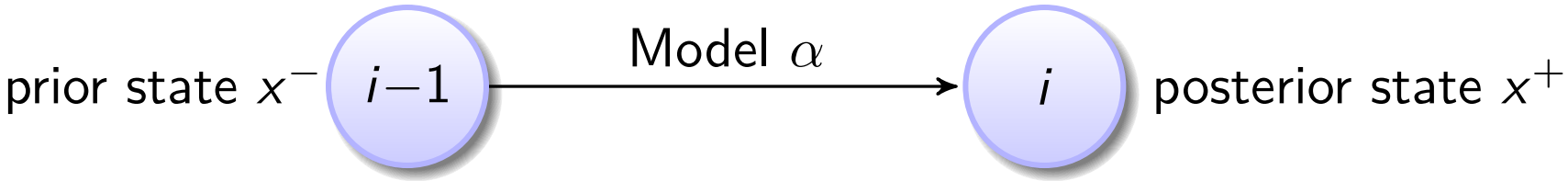
Real arithmetic: $F(x^-, x^+)$

check at runtime (efficient)

Provably Correct Synthesis of Monitors



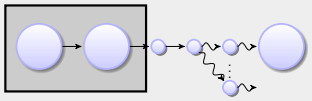
- Proof calculus of d$\mathcal{L}$ executes models symbolically



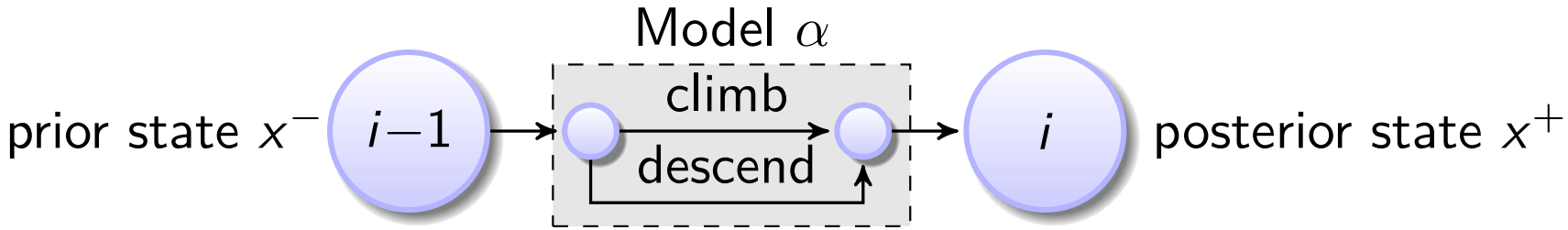
proof attempt

- $(x = x^-) \rightarrow \langle\alpha\rangle (x = x^+)$

Provably Correct Synthesis of Monitors



- Proof calculus of d$\mathcal{L}$ executes models symbolically

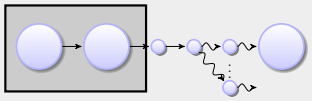


proof attempt

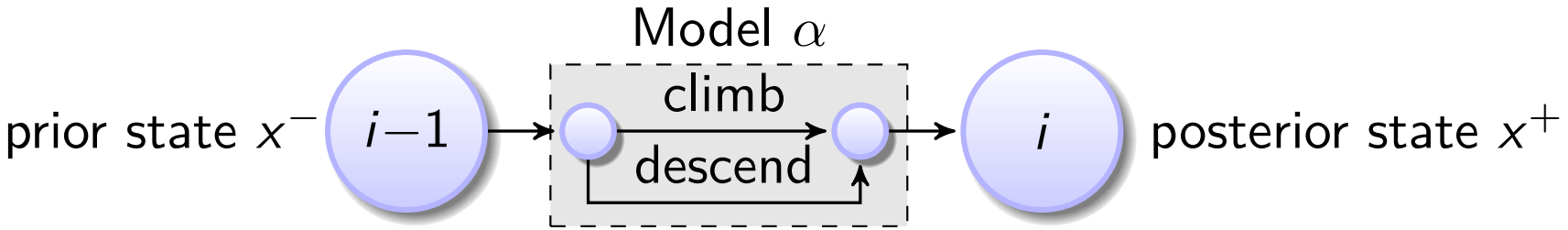
- $(x = x^-) \rightarrow \langle \text{climb} \cup \text{descend} \rangle (x = x^+)$

$$\langle \cup \rangle \frac{\langle \text{climb} \rangle \phi \vee \langle \text{descend} \rangle \phi}{\langle \text{climb} \cup \text{descend} \rangle \phi}$$

Provably Correct Synthesis of Monitors



- Proof calculus of d$\mathcal{L}$ executes models symbolically

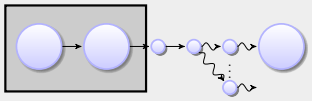


proof attempt

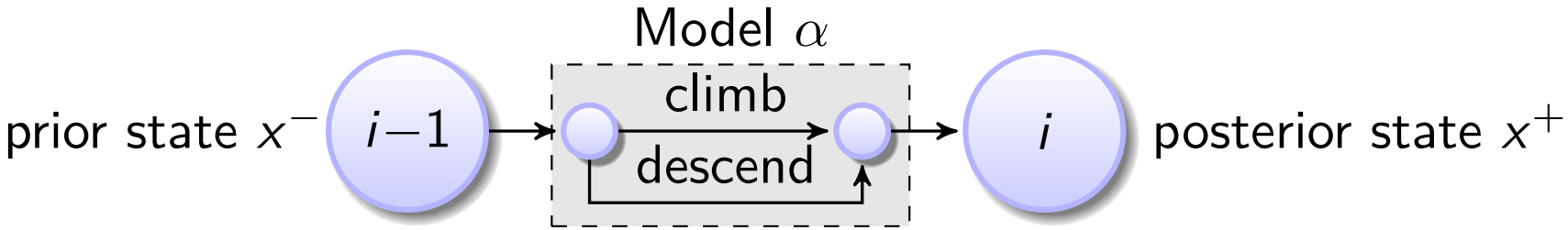
$$(x = x^-) \rightarrow \langle \text{climb} \cup \text{descend} \rangle (x = x^+)$$

$$\langle \text{climb} \rangle (x = x^+) \quad \vee \quad \langle \text{descend} \rangle (x = x^+)$$

Provably Correct Synthesis of Monitors



- Proof calculus of d$\mathcal{L}$ executes models symbolically



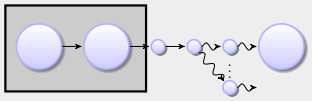
proof attempt

$$(x = x^-) \rightarrow \langle \text{climb} \cup \text{descend} \rangle (x = x^+)$$

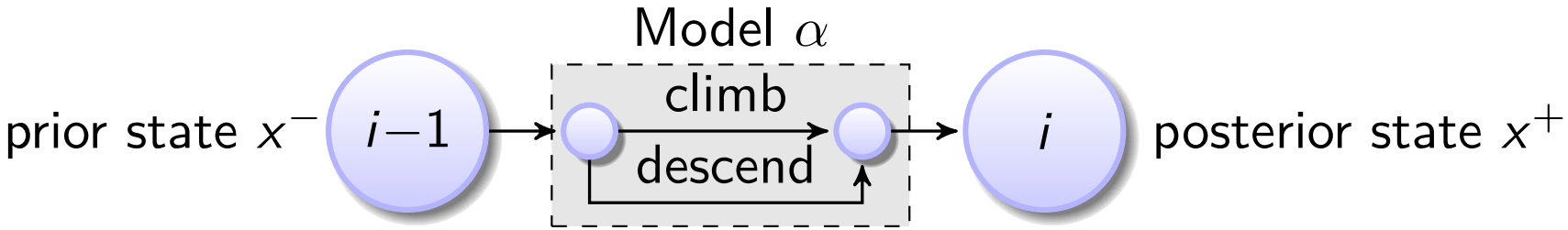
$$\langle \text{climb} \rangle (x = x^+) \quad \vee \quad \langle \text{descend} \rangle (x = x^+)$$

$$F_1(x^-, x^+) \qquad\qquad F_2(x^-, x^+)$$

Provably Correct Synthesis of Monitors



- Proof calculus of d$\mathcal{L}$ executes models symbolically



proof attempt

$$(x = x^-) \rightarrow \langle \text{climb} \cup \text{descend} \rangle (x = x^+)$$

$$\vee$$

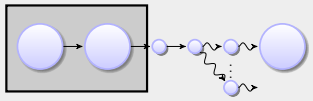
$$\langle \text{climb} \rangle (x = x^+) \qquad \langle \text{descend} \rangle (x = x^+)$$

$$F_1(x^-, x^+) \qquad F_2(x^-, x^+)$$

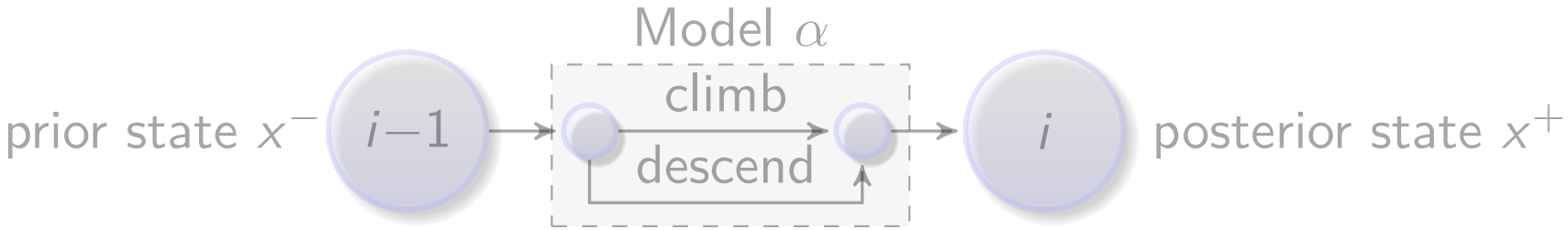
Monitor: $F_1(x^-, \overbrace{x^+) \vee F_2(}x^-, x^+)$

- The subgoals that cannot be proved express all the conditions on the relations of variables imposed by the model

Provably Correct Synthesis of Monitors



- Proof calculus of d$\mathcal{L}$ executes models symbolically



Model Monitor

Immediate detection of model violation

$\rightsquigarrow$ Mitigates safety issues with safe fallback action

$F_1(x^-, x^+)$ $F_2(x^-, x^+)$

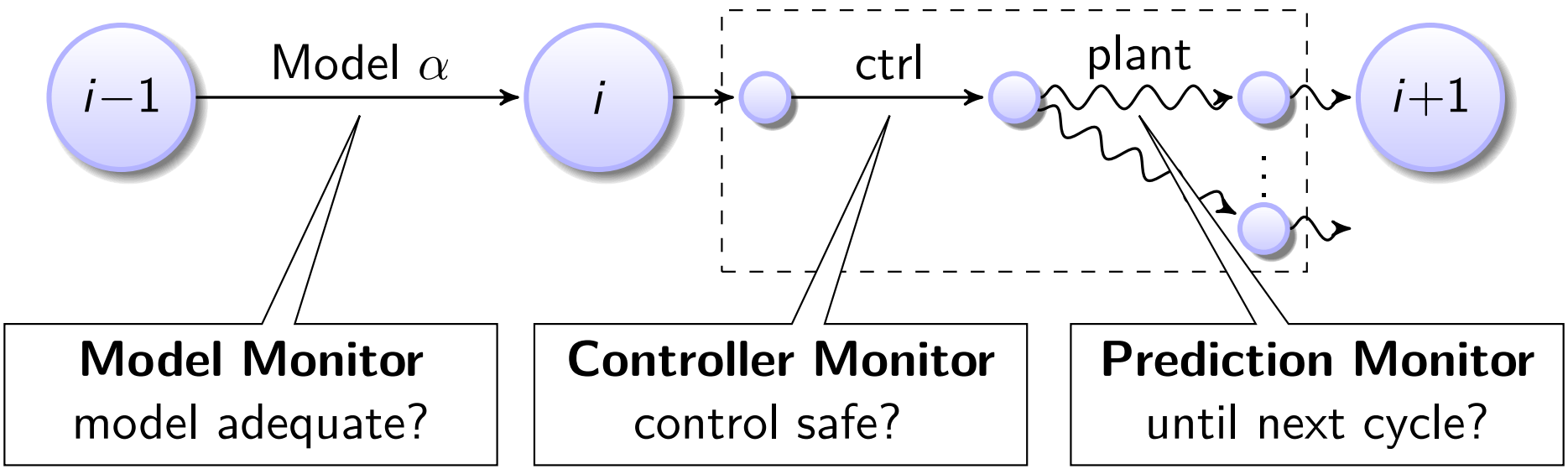
Monitor: $F_1(x^-, x^+) \vee F_2(x^-, x^+)$

- The subgoals that cannot be proved express all the conditions on the relations of variables imposed by the model

Conclusion

ModelPlex ensures that proofs apply to real CPS

- Validate model compliance
- Characterize compliance with model in logic
- Prover transforms compliance formula to executable monitor

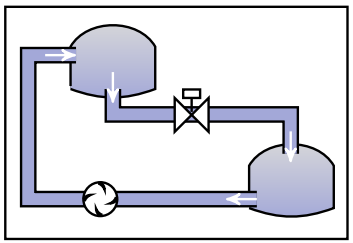


Thank You!

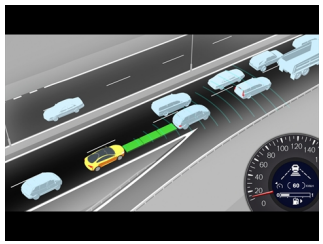
Evaluation

- Evaluated on hybrid system case studies

Water tank



Cruise control



© Volvo

Traffic control

© ASFINAG

Ground robots

© Black-I Robotics

Train control

© Harald Eisenberger

- Model sizes: 5–16 variables
- Monitor sizes: 20–150 operations (larger if automated simplification to remove redundant checks is computationally infeasible)
- Theorem: ModelPlex is decidable and monitor synthesis can be automated in important classes