(Belief)
Dynamic Doxastic Differential Dynamic Logic (d4L) for Belief-Aware Cyber Physical Systems

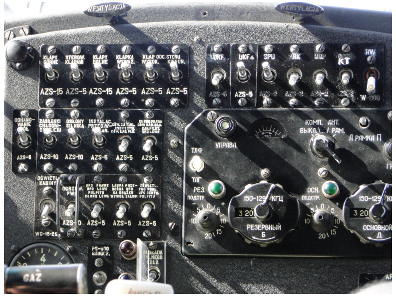
João G. Martins[1,2], André Platzer[2], João Leite[1]

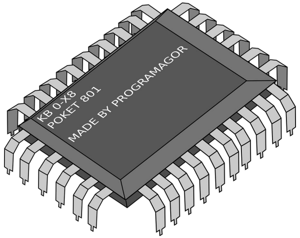
NOVALINCS [1]   Carnegie Mellon University [2]

Cyber-Physical Systems (CPS)

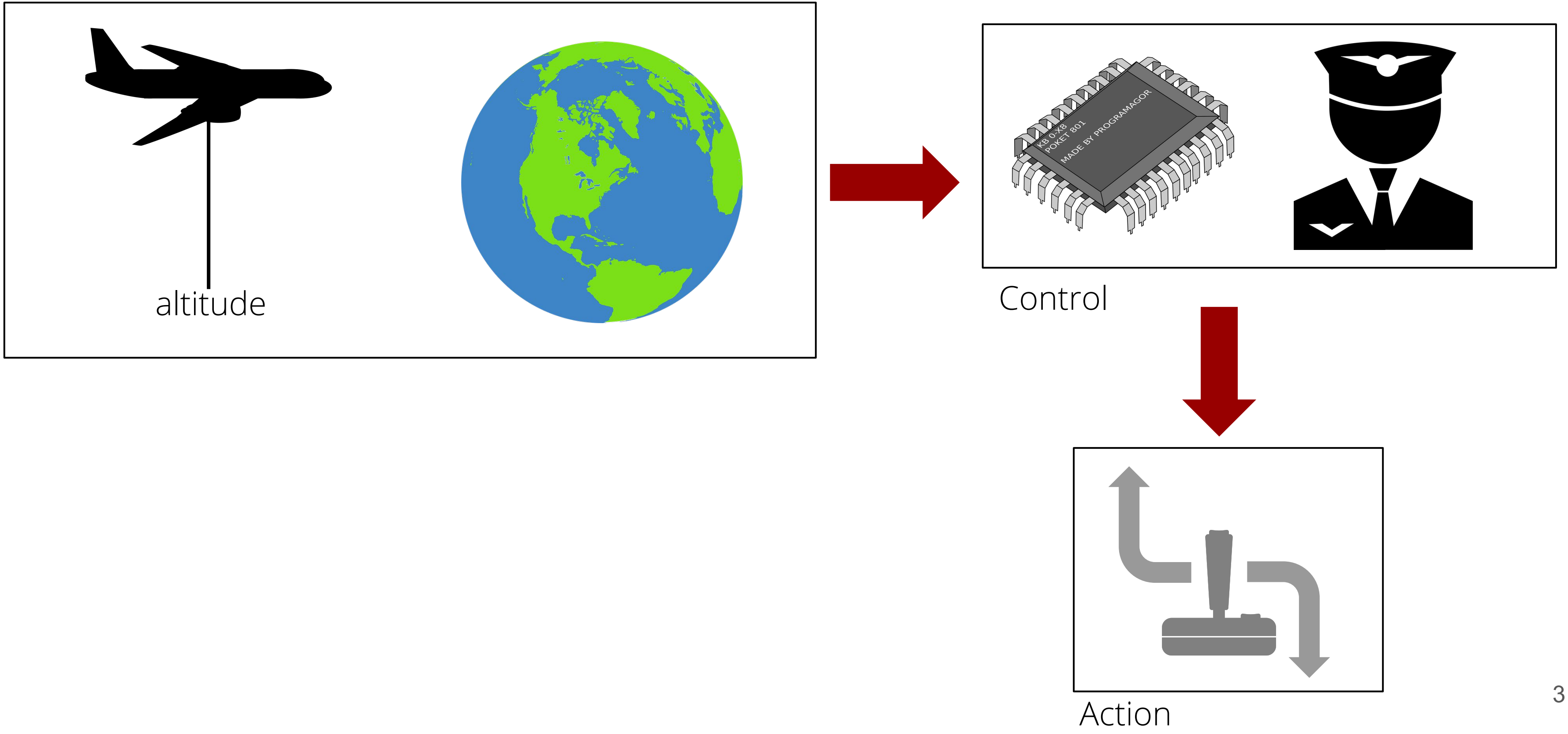
Continuous movement

Discrete control



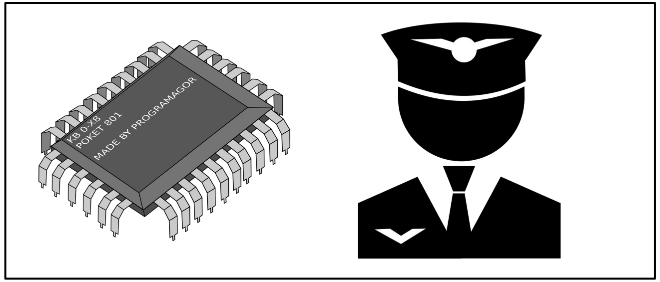


Belief-aware Cyber-Physical Systems

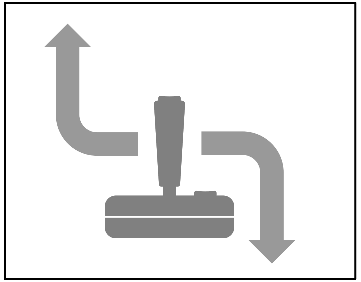


Belief-aware Cyber-Physical Systems

Information



Control



Action

- Sensors are noisy
- Incomplete information
- Imperfect information

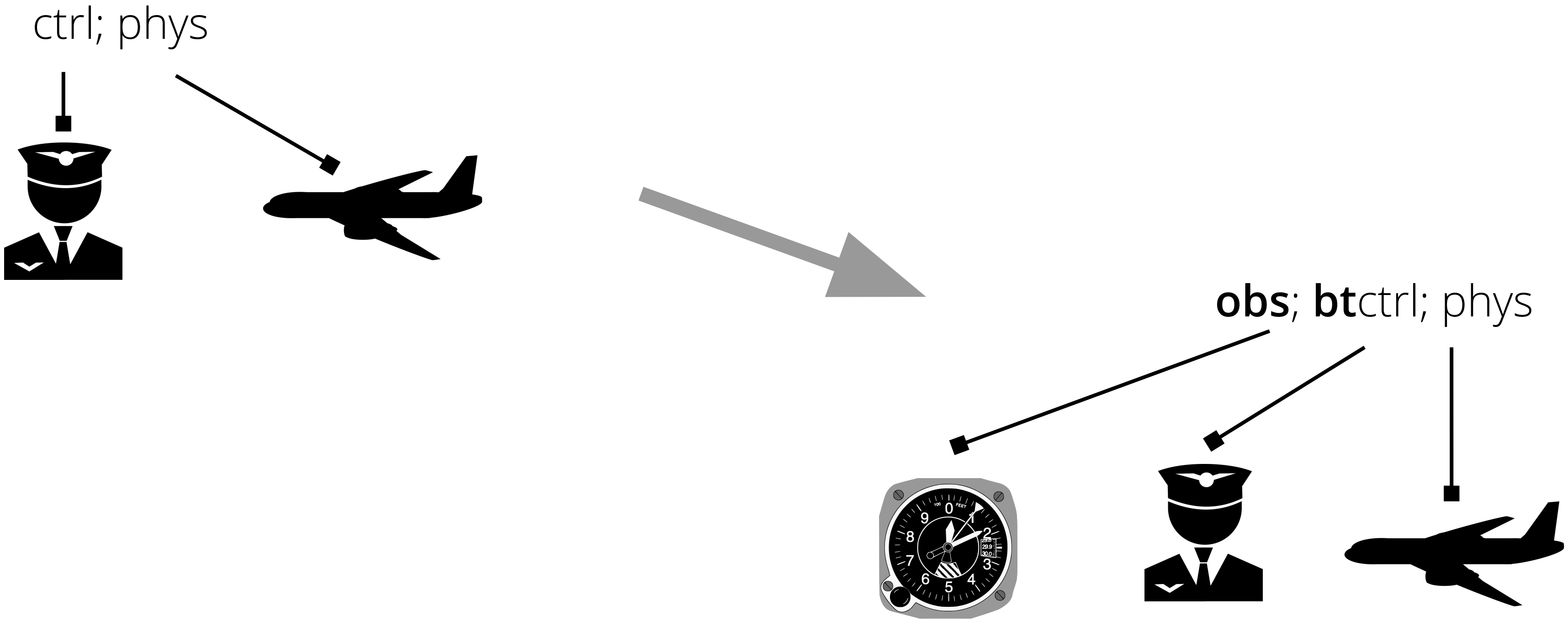
Belief-aware Cyber-Physical Systems

First principles approach

1. Real arithmetic
2. World change
3. Beliefs
4. Belief change
5. Sequent calculus

Belief-aware Cyber-Physical Systems

What we want



Belief-aware CPS Logic

Foundations: first order real arithmetic

Arithmetic operators:	$+, -, \times, \div$
Propositions:	$<, \leq, >, \geq, =$
Connectives:	$\wedge, \vee, \rightarrow, \neg$
Quantifiers:	$\forall, \exists$

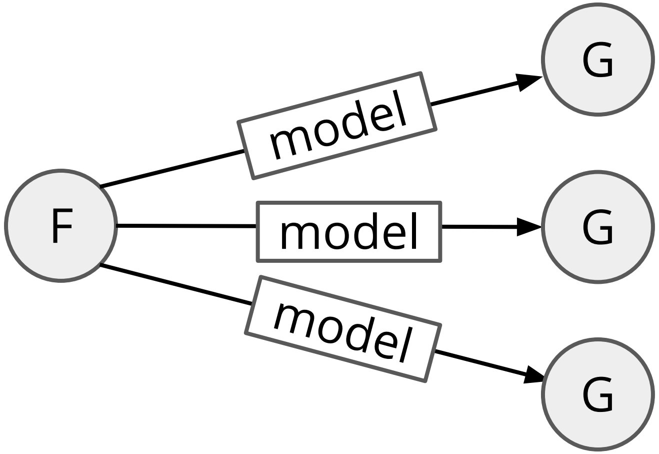
Belief-aware CPS Logic

Changing World

Syntax

F → [model] G

Semantics



Belief-aware CPS Logic

Changing World

Syntax

$x := \Theta$

$x' = f(x)$

$\alpha; \beta$

$\alpha \cup \beta$

$?F$

α^*

Belief-aware CPS Logic

Changing World

Syntax

autopilot := 1

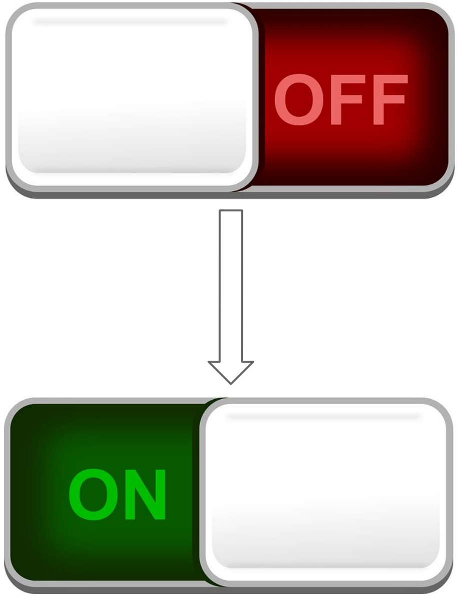
$x' = f(x)$

$\alpha; \beta$

$\alpha \cup \beta$

$?F$

α^*



Belief-aware CPS Logic

Changing World

Syntax

$x := \Theta$

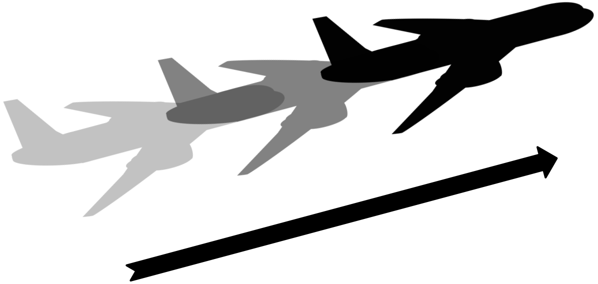
alt' = yvel

$\alpha; \beta$

$\alpha \cup \beta$

?F

α^*



Belief-aware CPS Logic

Changing World

Syntax

$x := \Theta$

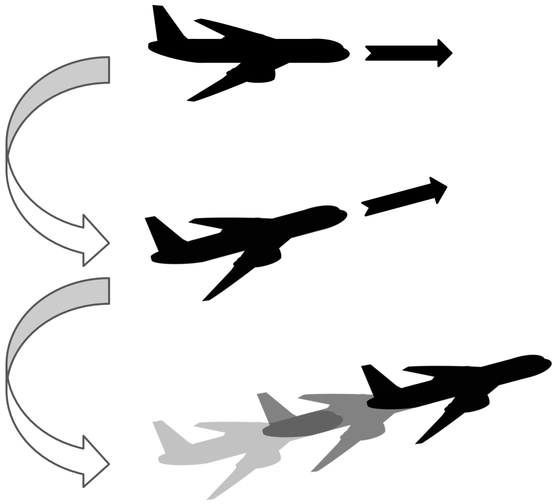
$x' = f(x)$

yvel := 1; alt' = yvel

$\alpha \cup \beta$

?F

α^*



Belief-aware CPS Logic

Changing World

Syntax

$x := \Theta$

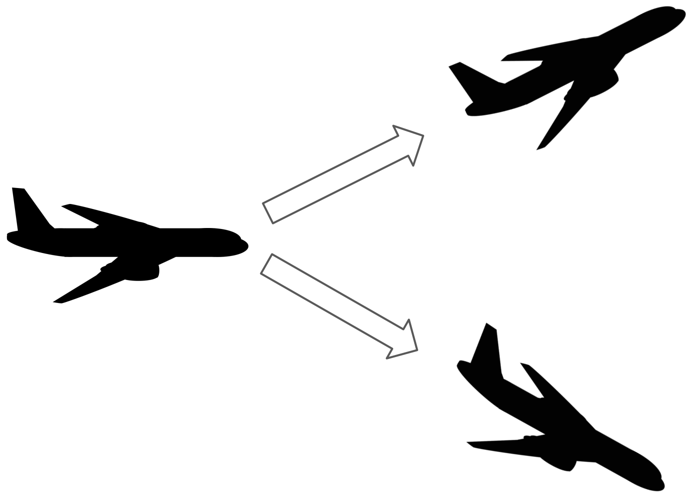
$x' = f(x)$

$\alpha; \beta$

yvel := 1 ∪ yvel := -1

?F

α^*



Belief-aware CPS Logic

Changing World

Syntax

$x := \Theta$

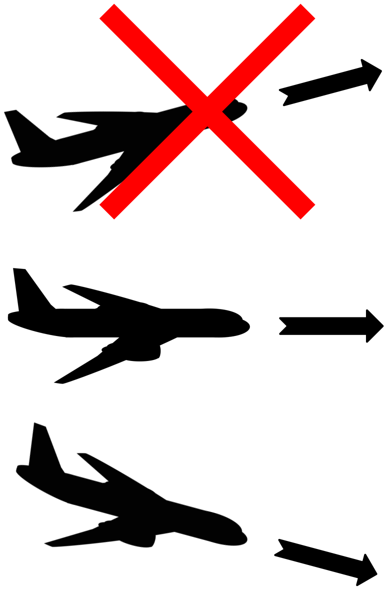
$x' = f(x)$

$\alpha; \beta$

$\alpha \cup \beta$

?yvel < 1

α^*



Belief-aware CPS Logic

Changing World

Syntax

$x := \Theta$

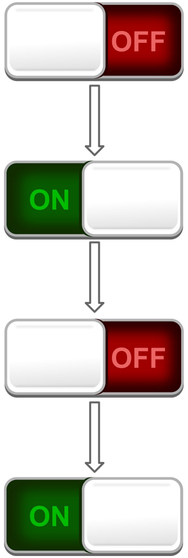
$x' = f(x)$

$\alpha; \beta$

$\alpha \cup \beta$

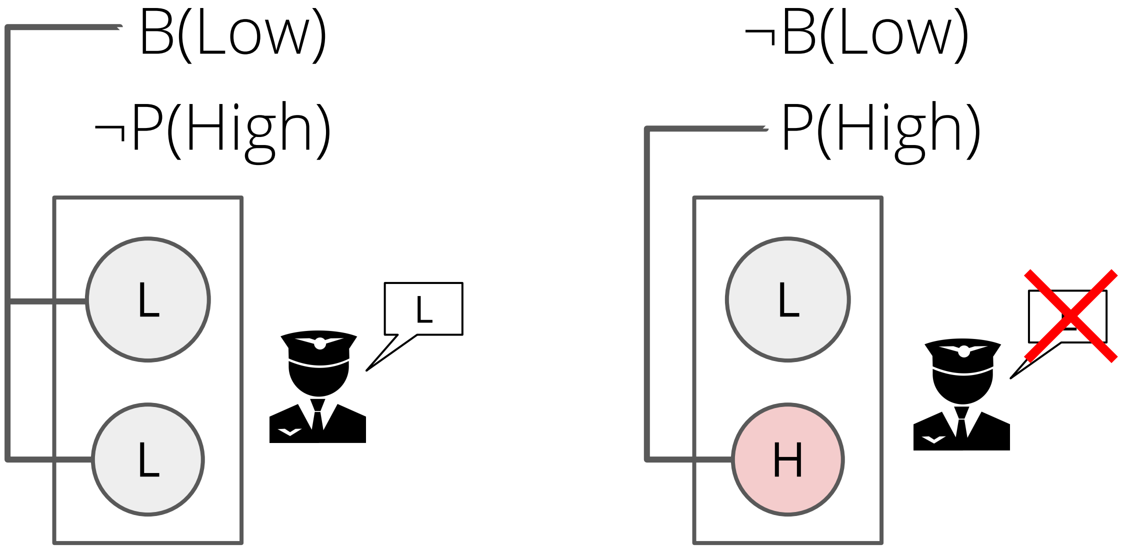
$?F$

(autopilot := 1 - autopilot)*



Belief-aware CPS Logic

Belief: possible world semantics



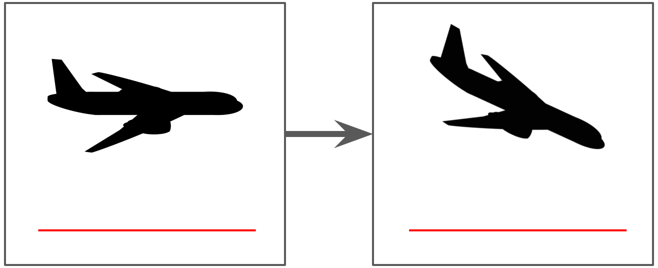
Belief-aware CPS Logic

Modalities: overview

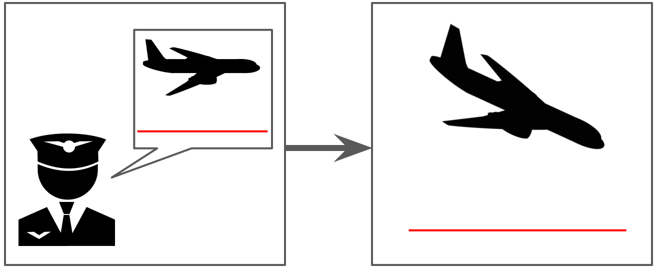
	Universal	Existential	Universe
Logical	$\forall$	$\exists$	Reals
Dynamic	$\Box$	$\Diamond$	Transitions
Doxastic	B	P	Possible worlds

Belief-aware CPS Logic

Belief-triggered control



?alt > 10; yinput := -1



?B(alt > 10); yinput := -1

Belief-aware CPS Logic

Belief: guiding principles

How to learn new information?

Belief-aware CPS Logic

Learning operator

$x := \Theta$

$x' = f(x)$

$\alpha; \beta$

$\alpha \cup \beta$

$?F$

α^*

$L(\alpha)$

$x_p := \Theta$

$\alpha; \beta$

$\alpha \cup \beta$

$?F$

Learning as a program

“Unified” language of change

Belief-aware CPS Logic

Learning operator

$L(\alpha)$

- Suspect α happened
- All outcomes of α possible
- World *does not change*

$\alpha; L(\alpha)$

Observable action

$L(\alpha \cup \beta)$

α or β: but which?

Belief-aware CPS Logic

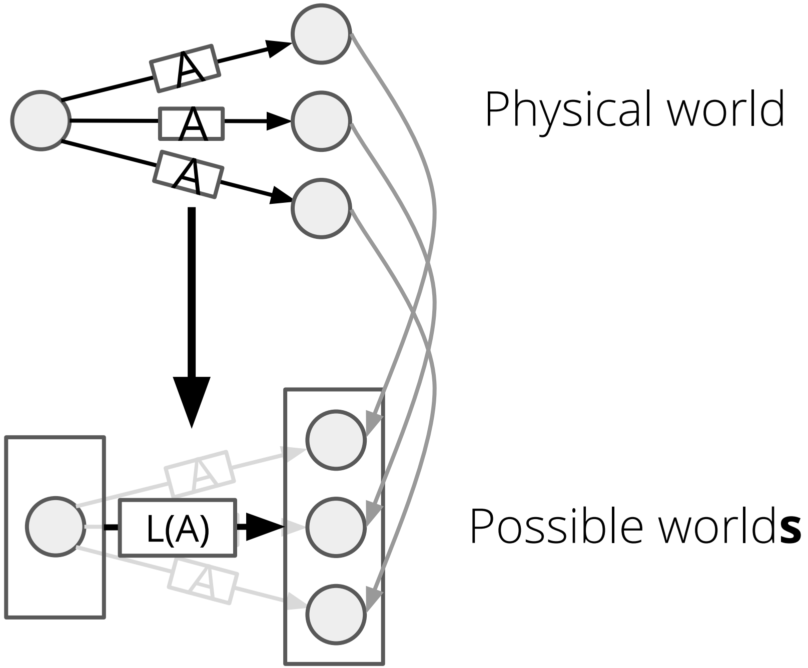
Learning operator

A

Transition-based change

Doxastic change

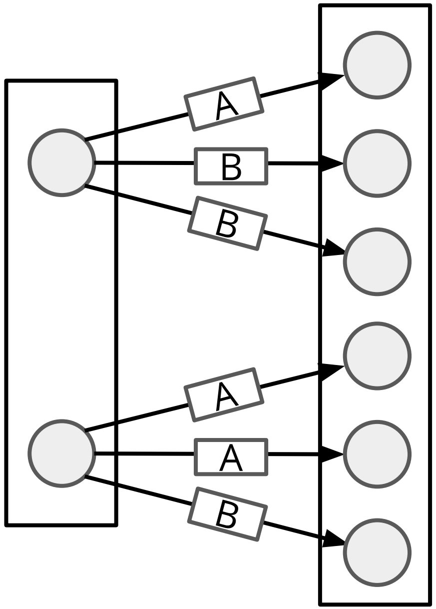
L(A)



Belief-aware CPS Logic

Learning new information

$[L(A \cup B)] F$

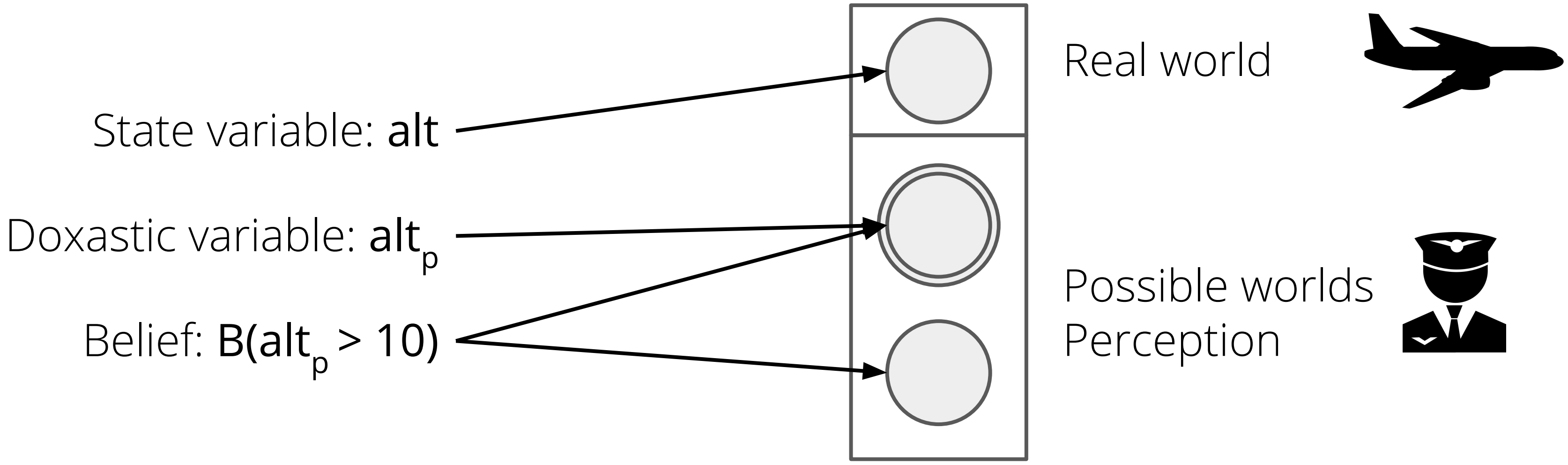


Multiple possible worlds

- Execute at each world
- All transition
- All outcomes indistinguishable

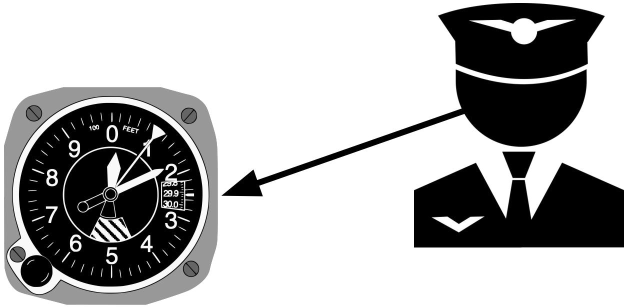
Belief-aware CPS Logic

Doxastic variables



Belief-aware CPS Logic

Learning and sensors



Perfect sensor

$L(?alt_p = alt)$

$L(alt_p := alt)$

Imperfect sensor

$L(?|alt_p - alt| < \varepsilon)$

Belief-aware CPS Logic

Calculus for belief change

Proof rules for learned programs

$x_p := \Theta$

$\alpha ; \beta$

$\alpha \cup \beta$

$?F$

Belief-aware CPS Logic

Calculus for belief change: assignment

Sound rule

$$\frac{C \vdash F(\Theta)}{C \vdash [L(x_p := \Theta)]\ F(x_p)}$$

- Syntactic substitution = semantic substitution
- Under admissibility
- Technically complex

Belief-aware CPS Logic

Calculus for belief change: sequential composition

Sound rule

$$\frac{C \vdash [L(\alpha) \,;\, L(\beta)]\, F}{C \vdash [L(\alpha \,;\, \beta)]\, F}$$

- Reduced to non-learned sequential composition

Belief-aware CPS Logic

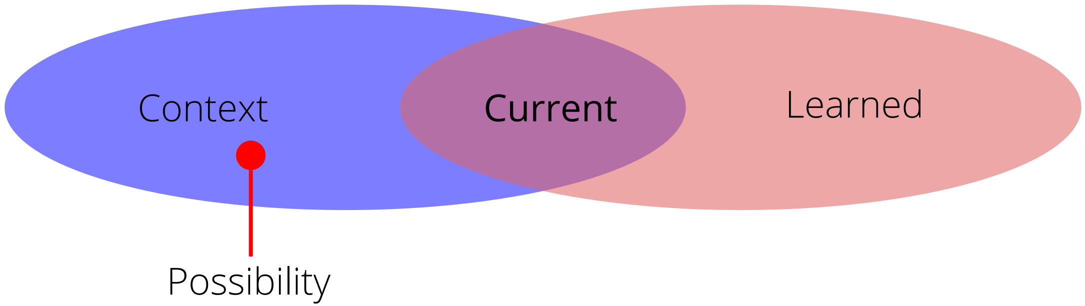
Calculus for belief change: test

~~Sound~~ rule

$$\frac{C \vdash B(F) \rightarrow G}{C \vdash [L(?F)]G}$$

Sound rule

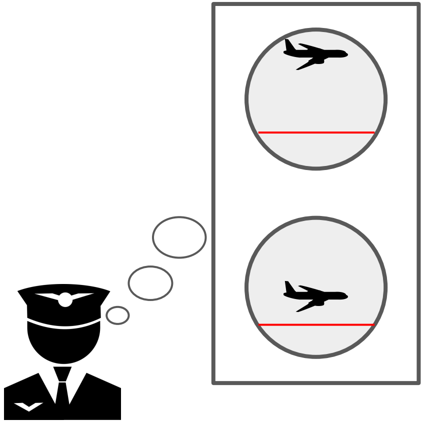
$$\frac{C_B, C_R \vdash B(F) \rightarrow G}{C_B, \mathbf{C_P}, C_R \vdash [L(?F)]G}$$



Belief-aware CPS Logic

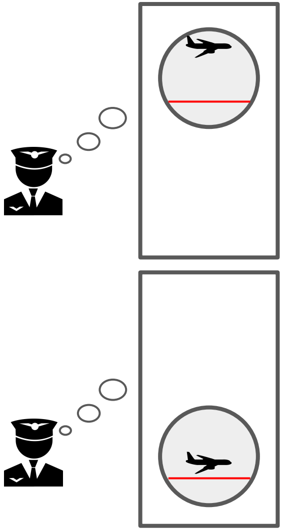
Calculus for belief change: choice

L(?high ∪ ?low)



$L(\alpha \cup \beta) \neq L(\alpha) \cup L(\beta)$

L(?high) ∪ L(?low)



Belief-aware CPS Logic

Calculus for belief change: choice

Traditional choice rules

$$\frac{C \vdash [\alpha]\, F \land [\beta]\, F}{C \vdash [\alpha \cup \beta]\, F}$$

$$\frac{C \vdash \langle\alpha\rangle\, F \lor \langle\beta\rangle\, F}{C \vdash \langle\alpha \cup \beta\rangle\, F}$$

No longer work
Need case distinction

Belief-aware CPS Logic

Calculus for belief change: choice

Most conservative of:
- Dynamic modality
- Doxastic modality

Sound rules

$$\frac{C \vdash [L(\alpha)]\, B(F) \wedge [L(\beta)]\, B(F)}{C \vdash [L(\alpha \cup \beta)]\, B(F)} \quad []B,\ []P,\ \langle\rangle B$$

$$\frac{C \vdash \langle L(\alpha)\rangle\, P(F) \vee \langle L(\beta)\rangle\, P(F)}{C \vdash \langle L(\alpha \cup \beta)\rangle\, P(F)} \quad \langle\rangle P$$

Belief-aware CPS Logic

Calculus for belief change

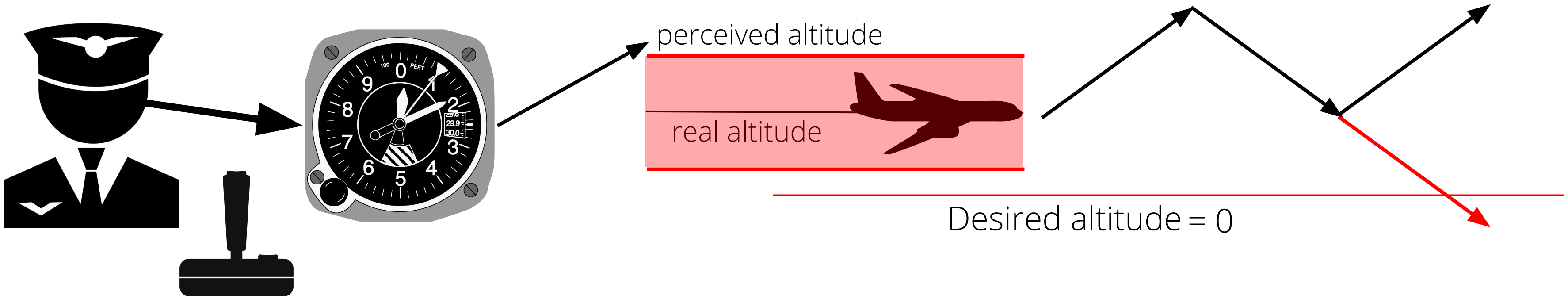
Theorem: the calculus for world change is sound. [1]

Theorem: the calculus for belief change is sound.

[1] Platzer, A.: Differential dynamic logic for hybrid systems. J. Autom. Reas. 41(2), 143–189 (2008)

Case study: altitude control

Overview

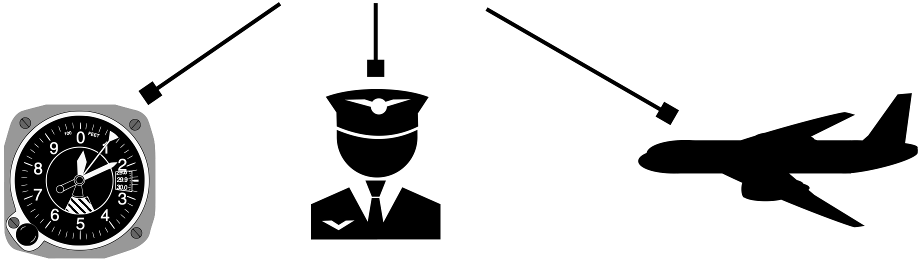


Case study: altitude control

A new standard pattern

Safety

pre → [(obs; btctrl; phys)*] safe



Case study: altitude control

Full model

$T > 0 \land alt > 0 \land \varepsilon > 0 \rightarrow [($

obs —— $L(?alt_p - alt < \varepsilon);$

btctrl —— $?B(alt_p - T - \varepsilon > 0); \mathbf{yv} := -1 \cup ?P(alt_p - T - \varepsilon \leq 0); \mathbf{yv} := 1$

phys —— $t := 0; t' = 1, alt' = \mathbf{yv} \; \& \; t < T$

$)^*] \; alt > 0$

✓ verified

Case study: altitude control

Devil's advocate: modeling trick

$T > 0 \land alt > 0 \land \varepsilon > 0 \rightarrow [($

obs —— $L(?alt_p - alt < \varepsilon);$

btctrl —— $?B(alt_p - T - \varepsilon > 0); yv := -1 \cup ?P(alt_p - T - \varepsilon \leq 0); yv := 1$

phys —— $t := 0; t' = 1, alt' = yv \;\&\; t < T$

$)^*] \; alt > 0$

Case study: altitude control

Modeling trick: limitations

Relies on modal resolution of nondeterminism

- Only for safety □, not liveness ◊

Changes arithmetic

- $?P(alt_p - T - \varepsilon > A)$ becomes $?alt_p - T + \varepsilon > A$
- Obscures doxastic intuitions
- Quickly becomes complex

Conclusion

d4L: a logic for verifying belief-aware CPS

Theoretical

- Semantics for changing belief in a changing world
- General learning operator
- Sequent calculus in the reals

Practical

- Belief-triggered controllers
- First principles verification for belief-aware CPS

Thank you

Questions?

Appendix

Suggested questions ;)

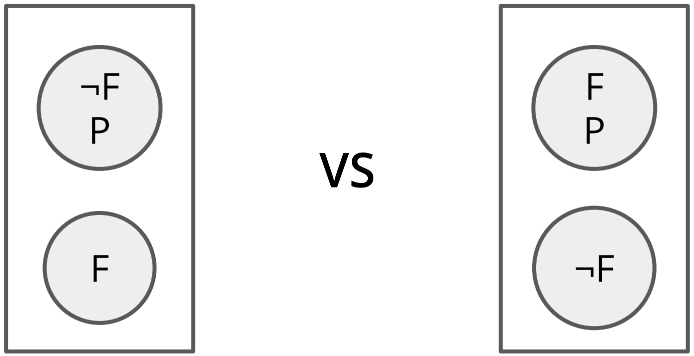
- Test, possibility & completeness
- Beliefs about beliefs
- Repeated contraction of possible worlds
- Learning in uncountable domains
- Doxastic assignment, $x_p := \Theta$ vs $x := \Theta$
- Learning operator semantics

Appendix

Possibility & completeness

$$\frac{C_B, C_R \vdash B(F) \rightarrow G}{C_B, \mathbf{C_P}, C_R \vdash [L(?F)]G}$$

Hard to know
which P to keep



Appendix

Belief: requirements

Desired axiom

$B_a(F) \rightarrow [L_b(\alpha)]\, B_a(F)$

Impossible in Kripke models

No calculus, but easy semantics

Appendix

Belief: contraction of possible worlds

Nondeterministic assignment

$x := * \quad \equiv \quad x' = 1;\ x' = -1$

Nondeterministic doxastic assignment

$x_p := *$

$L(x_p := *;\ ?F(x_p))$

Appendix

Learning in uncountable domains

Action model/Epistemic actions

$$[A,e]G \leftrightarrow \bigwedge_{eRf} [A,f]G$$

Conjunction of all possible worlds

- Impossible for reals

Appendix

Doxastic assignment vs regular assignment

Unsound proof rule

$$\frac{C \vdash [L(x := \Theta) \; ; \; L(\beta(x))] \; F}{C \vdash [L(x := \Theta; \; \beta(x))] \; F}$$

Still unsound proof rule

$$\frac{C \vdash [L(x := \Theta) \; ; \; L(\beta(x_p))] \; F}{C \vdash [L(x := \Theta; \; \beta(x))] \; F}$$

Appendix

Learning operator semantics

- $(\omega, \omega') \in \rho_\eta(L(\gamma))$ *if:* $r' = r$, $W' = \{\nu : \textit{there is } t \in \omega \textit{ s.t. } (\omega \oplus t, \nu) \in \rho_\eta(\gamma)\}$, $\omega'(\nu) = \mathrm{DV}(\nu)$ *for all* $\nu \in \omega'$, *and* $\mathrm{DW}(\mathrm{DW}(\omega')) = \mathrm{DW}(\omega)$.