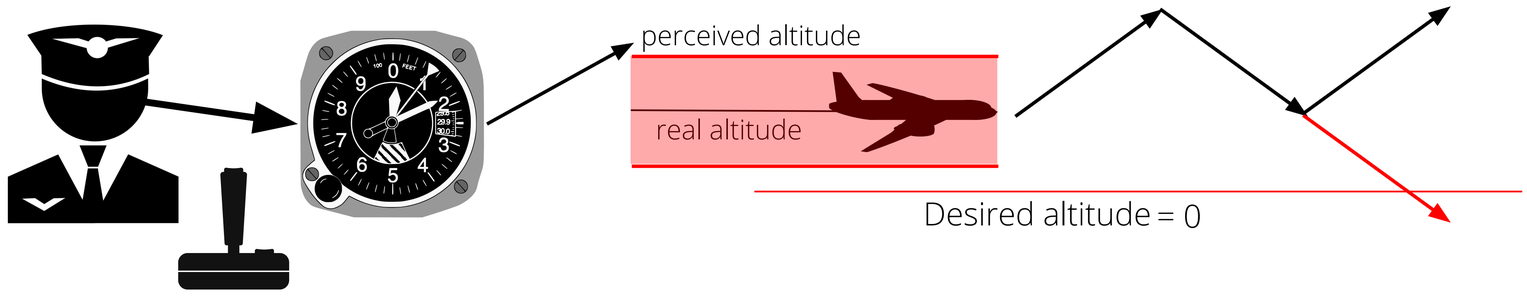
BELIEF-AWARE CYBER-PHYSICAL SYSTEMS

André Platzer (PI), João Martins

Carnegie Mellon University

Case study: belief-triggered altitude control

Pilot reads **altimeter**, which provides **noisy** information. **Beliefs**, newly **learned** by the pilot, **trigger** descent or climb **actions**.



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

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

Observation states that perceived and real altitude cannot differ by much.

Descent is **triggered** by the **Belief** that distance travelled and **worst-case noise** keep the airplane above ground. The mere **Possibility** of danger triggers a climb.

The plane moves in real time according to simplified **physics**.

$x := *$	Assign any $\mathbb{R}$ to x non-deterministically
$\alpha \cup \beta$	Run α or β non-deterministically
$?\phi; \alpha$	If condition ϕ is met, then run α
$L_p(\alpha)$	Pilot learns program α executed

Belief: subtler than expected

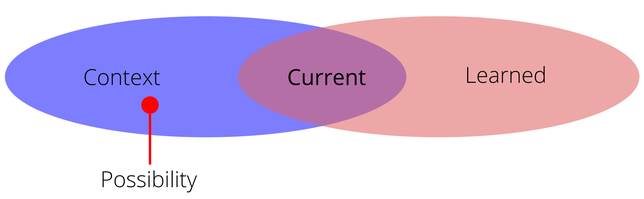
Learning that F must be true now is the same as believing that F must be true *a priori*.

~~Sound~~ rule

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

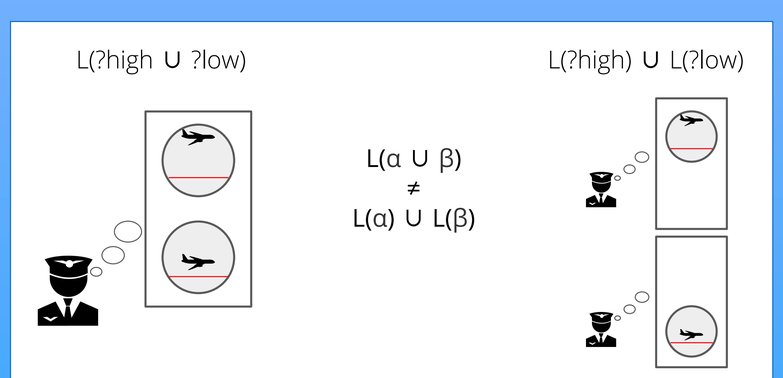
Sound rule

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



However, *learning deletes possibilities*, and without taking this into account, the calculus becomes **unsound**.

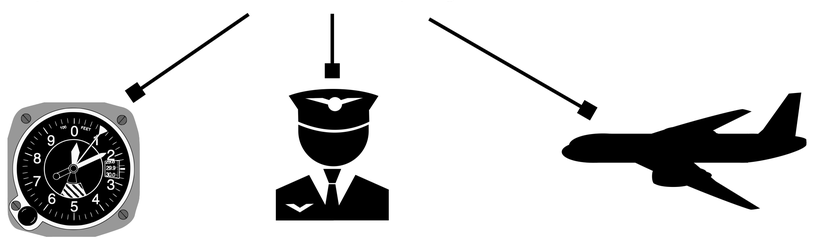
Learning about two possibilities is different than two possibilities for learning!



Progress: case study

Theorem: the calculus for belief-aware CPS sound.

$$pre \rightarrow [(\mathbf{obs}; btctrl; phys)^*] safe$$



The calculus enables the verification of CPS case studies.

- New paradigm, new model with explicit observation.
- Belief -> pilot decisions -> plane behavior -> learning -> belief. Everything is **interleaved**.
- **Modular** safety proofs: belief-only sections, real-world-only sections, little “glue” between the two.
- “Meta-properties” constraining what is believed and what is true become critical to the safety argument.