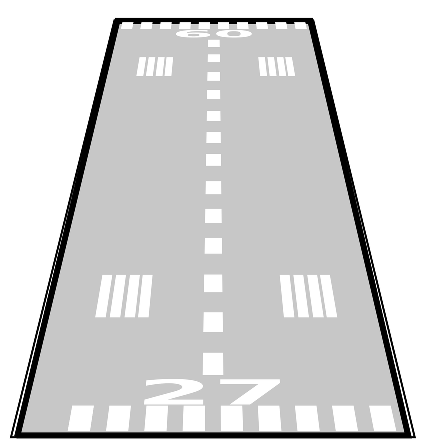
KNOWLEDGE-AWARE CYBER-PHYSICAL SYSTEMS

André Platzer (PI), João Martins
Carnegie Mellon University

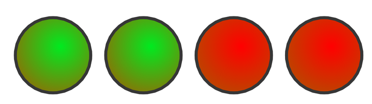
NSF CNS-1446712

Stepping up to AF-447: Precision Approach Path Indicator (PAPI)

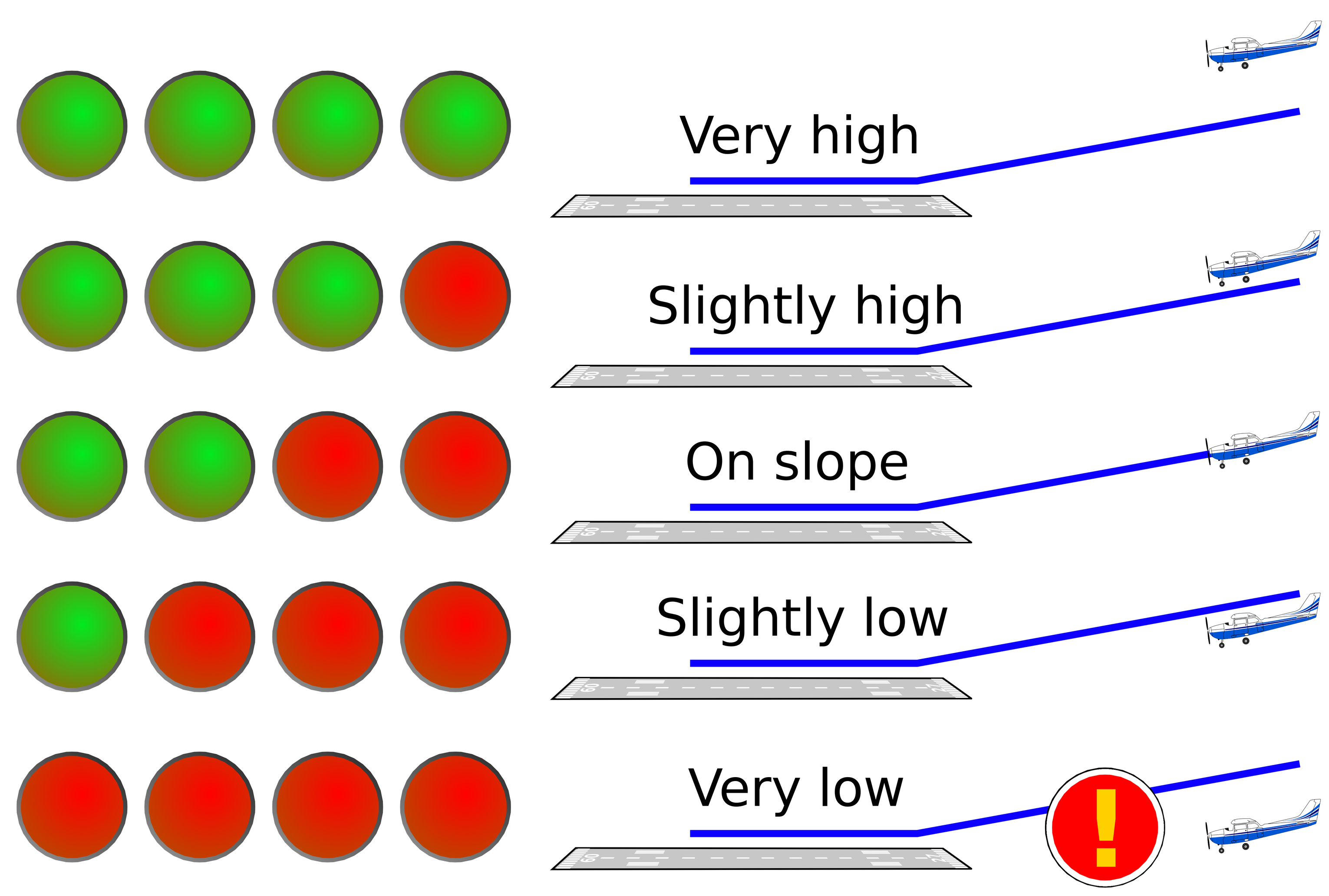
PAPI Description



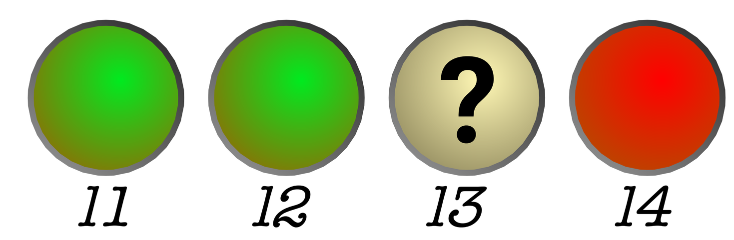
Four lights next to the runway indicate where aircraft are on the glide-path



Different patterns indicate 5 possible states



Challenge



$$L\left(\texttt{l1} := G; \texttt{l2} := G; \overbrace{(\texttt{l3} := G \cup \texttt{l3} := R)}^{\text{uncertainty}}; \texttt{l4} := R\right)$$

Poor visibility conditions or malfunction!
What should pilot training and policy be?

Encoding Safe Policy

$$\Big(((?d > obs; \texttt{learn-most}) \cup (?d \le obs; \texttt{learn-all}));$$
$$\texttt{decision-procedure};$$
$$\texttt{physics; light-upd}\Big)^*$$

1. If too far (d > obs), third light can't be identified
2. Pilot decides what to do given beliefs
3. Physics advances, glide path determines lights

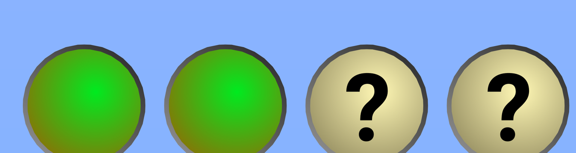
$\alpha \cup \beta$	Run either program non-deterministically
$?\phi; \alpha$	Check if condition is met, then run program
$L(\alpha)$	Pilot learns program executed
$[\alpha]\,\phi$	After all program runs, property holds

$$safe \rightarrow [\texttt{prog}]\, safe$$

Belief-Triggered Control

A glide path is safe when the airplane is cannot be low

$$safe\text{-}glidepath \equiv \texttt{l1} = G \land \texttt{l2} = G$$



A cautious pilot will climb when not certain of a safe glide path

$$?\left(\neg B\left(safe\text{-}glidepath\right)\right); yinput := 1$$

A reckless pilot will climb only when certain of an *unsafe* glide path

$$?\left(B\left(\neg safe\text{-}glidepath\right)\right); yinput := 1$$

Explicit beliefs encourage deeper understanding and granularity

$$\begin{aligned}
&?\left(\neg B\left(\texttt{l1} = G \land \texttt{l2} = G\right)\right); yinput := 1 \cup\\
&?\left(B\left(\texttt{l1} = G \land \texttt{l2} = G\right) \land \neg P\left(\texttt{l4} = G\right)\right); yinput := 0 \cup\\
&?\left(B\left(\texttt{l1} = G \land \texttt{l2} = G\right) \land P\left(\texttt{l4} = G\right)\right); yinput := -0.5 \cup\\
&?\left(B\left(\texttt{l1} = G \land \texttt{l2} = G\right) \land B\left(\texttt{l4} = G\right)\right); yinput := -1
\end{aligned}$$

Progress: Proof Contexts

Proof contexts Γ become challenging with changing beliefs

$$\frac{\Gamma \vdash B(\phi) \rightarrow \psi}{\Gamma \vdash [L(?\phi)]\,\psi}\;([]L?)$$

This intuitive rule looks innocent.
With changing belief, it's unsound!

A counter-example shows that P(x >1) should not remain.

$$\frac{P(x > 1) \vdash B(x = 1) \rightarrow P(x > 1)}{P(x > 1) \vdash [L(?x = 1)]\,P(x > 1)}$$

Learning a test program *contracts* possible worlds, which:
- Eliminates possibility
- Maintains beliefs

$$\frac{\Gamma_R, \Gamma_B \vdash B(\phi) \rightarrow \psi}{\Gamma_R, \Gamma_B, \Gamma_P \vdash [L(?\phi)]\,\psi}\;([]L?)$$