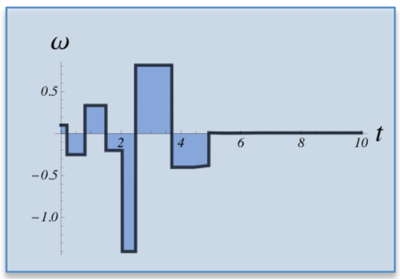
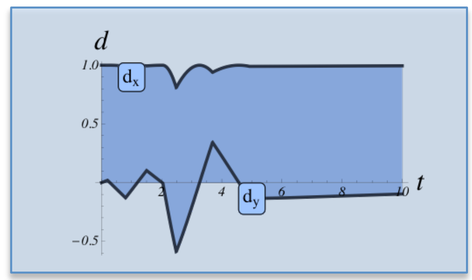
Safe Obstacle Avoidance of Autonomous Robotic Ground Vehicles



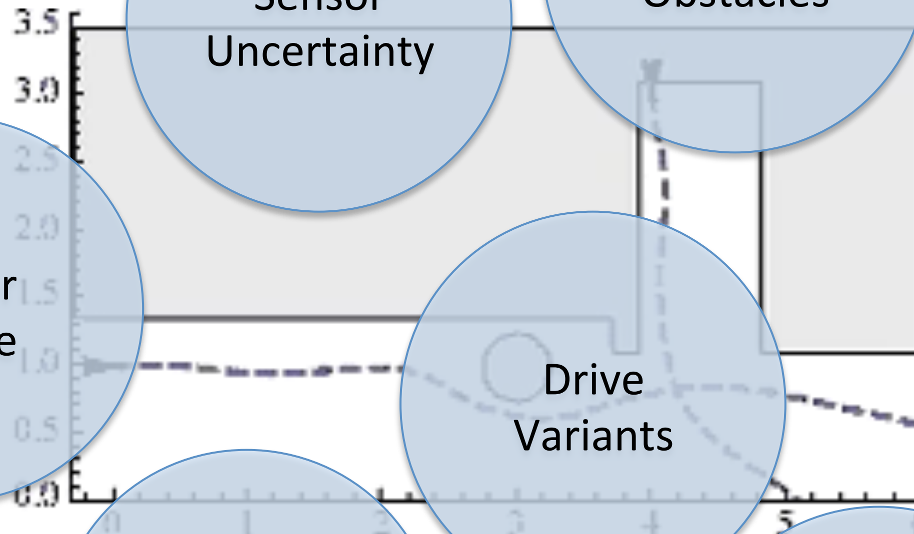


Stefan Mitsch, Khalil Ghorbal and **André Platzer**

Computer Science Department

Carnegie Mellon University

.:: Obstacle Avoidance



Stationary Obstacles

Sensor Uncertainty

Moving Obstacles

Obstacle Shape

Sensor Failure

Drive Variants

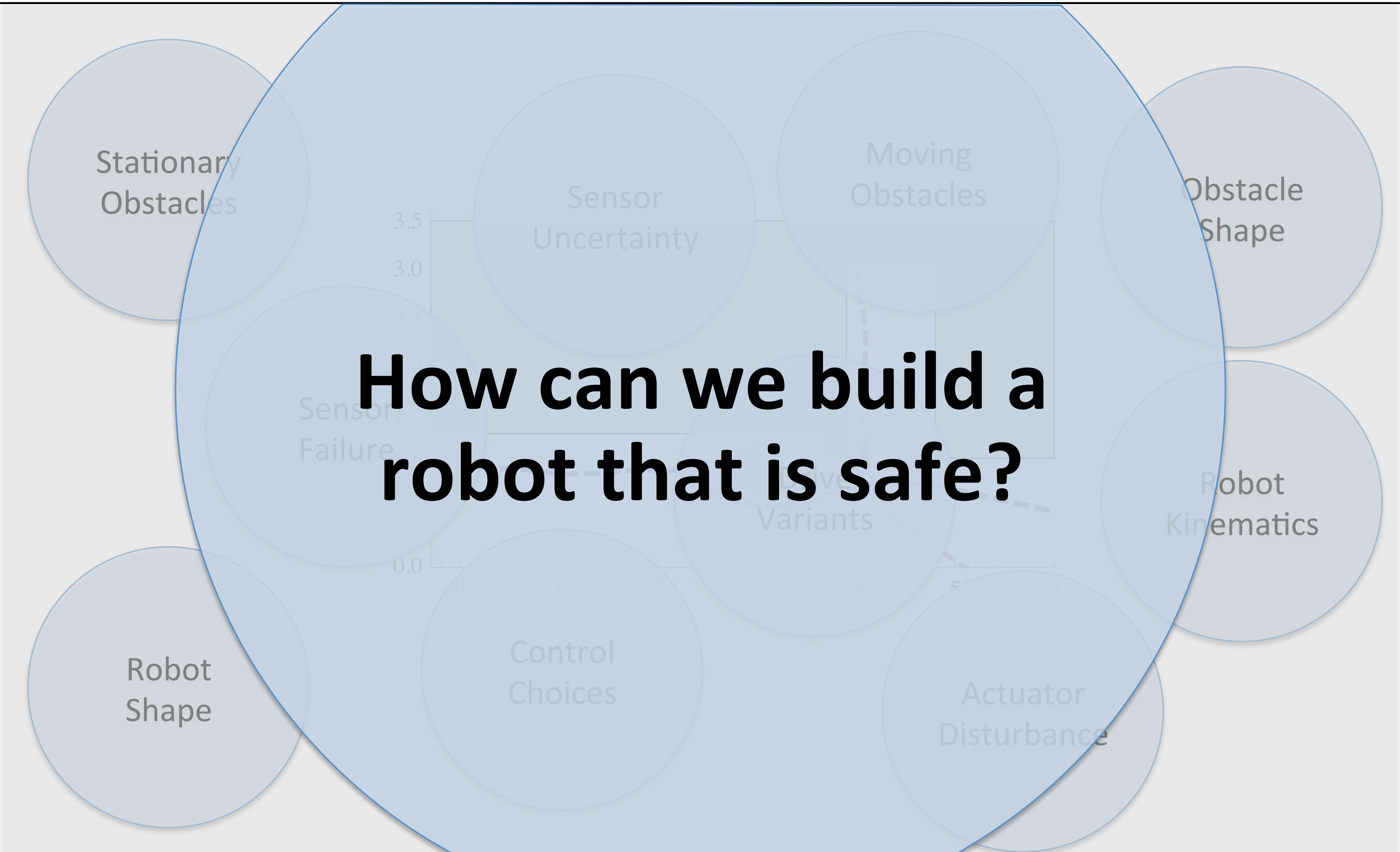
Robot Kinematics

Robot Shape

Control Choices

Actuator Disturbance

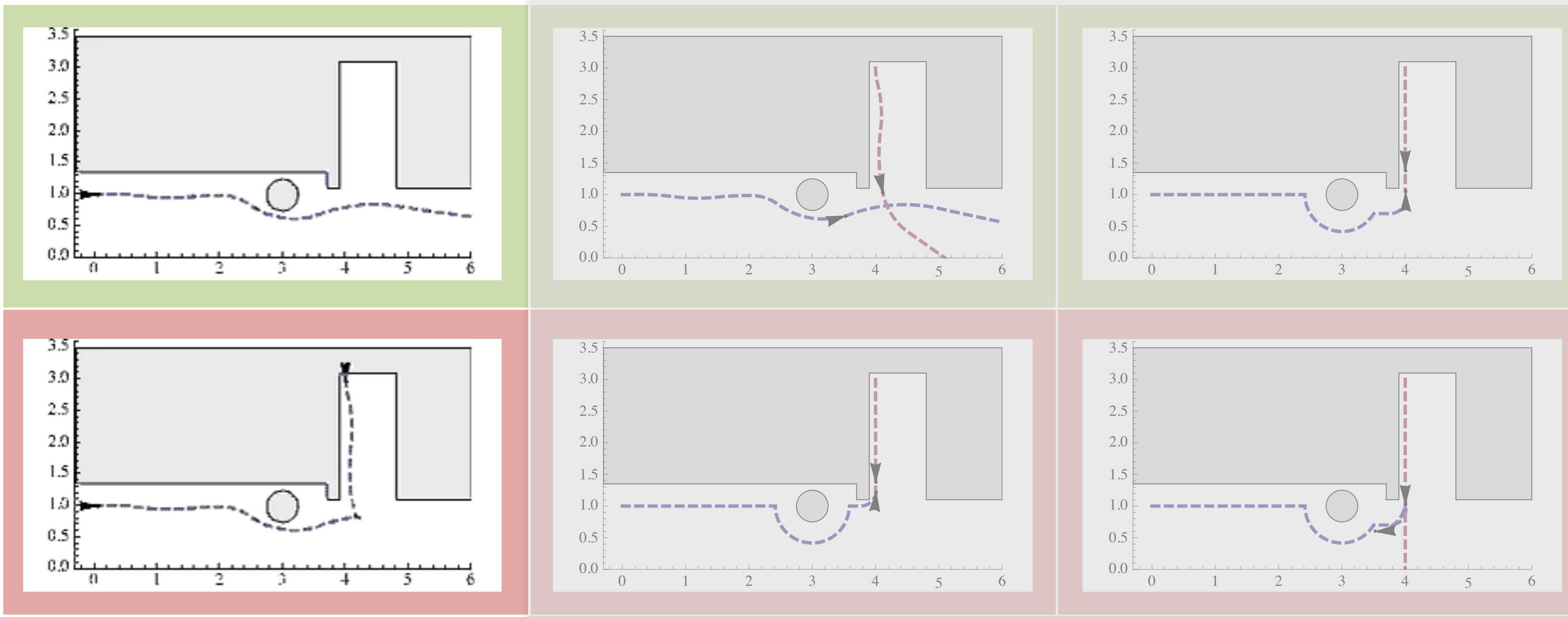
.:: Obstacle Avoidance



.:: Obstacle Avoidance

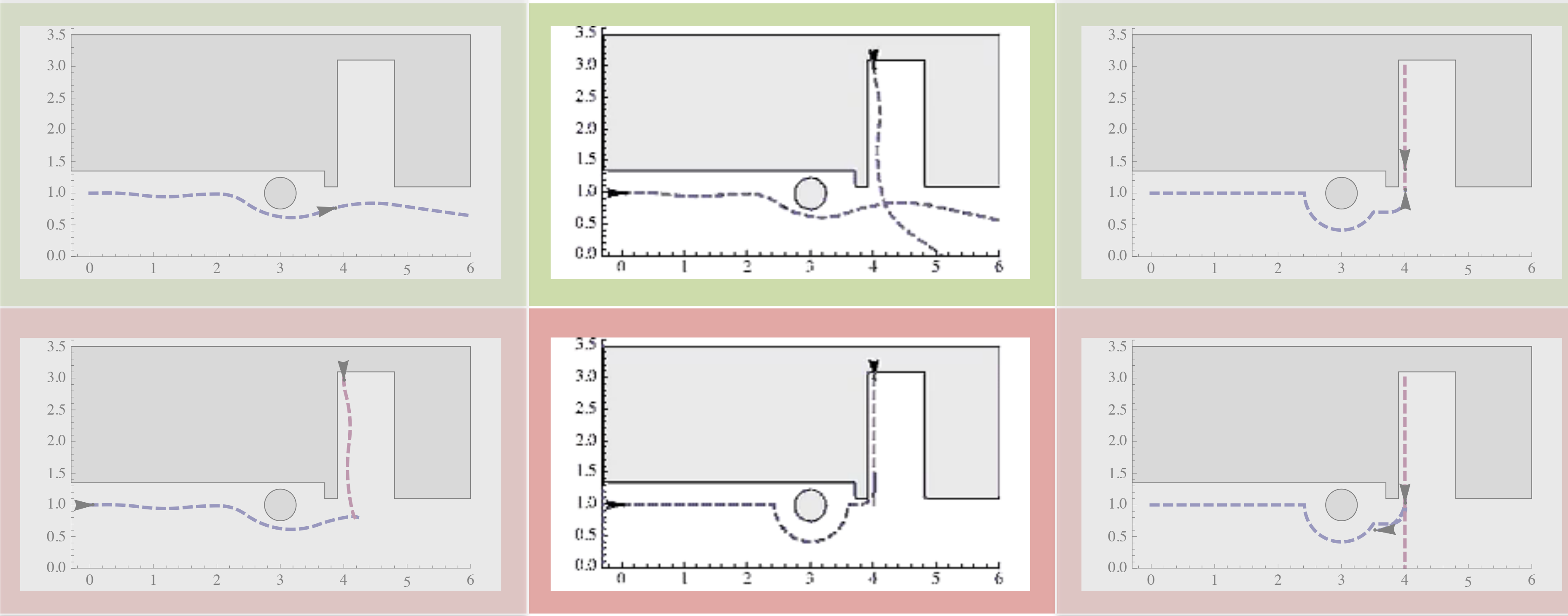
.:: Safety Definitions

Static safety	Passive safety	Passive friendly safety

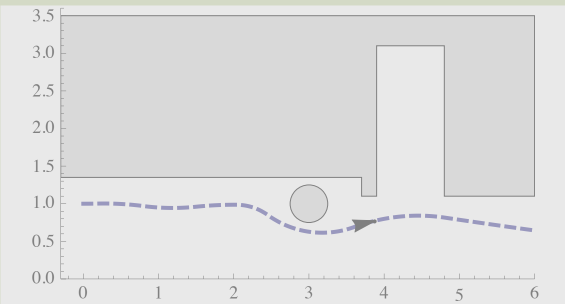
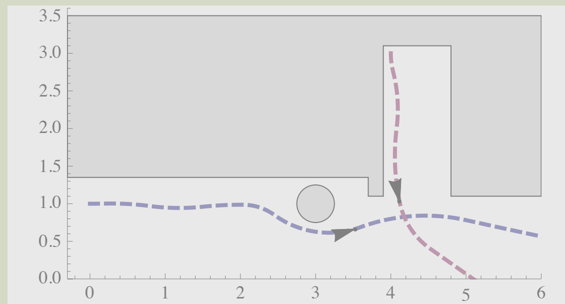
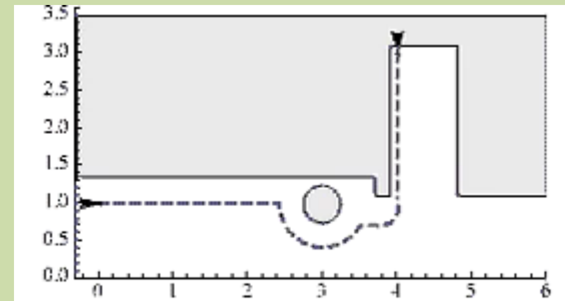
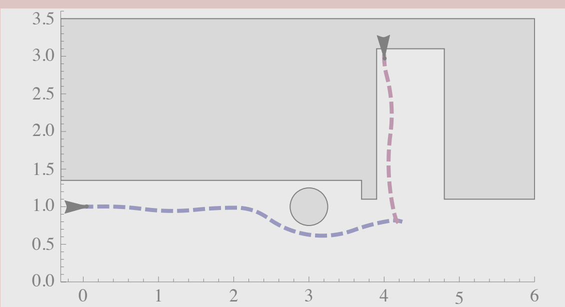
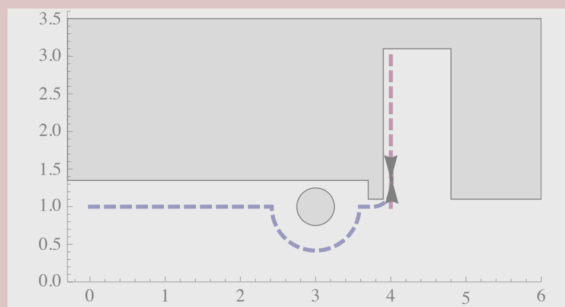
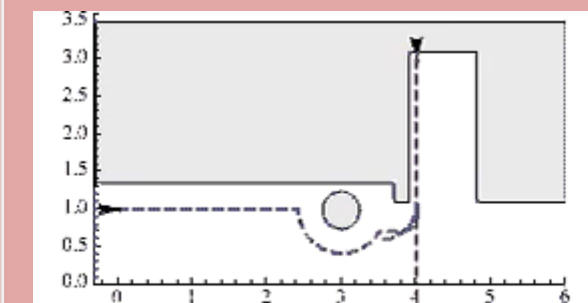


.:: Safety Definitions

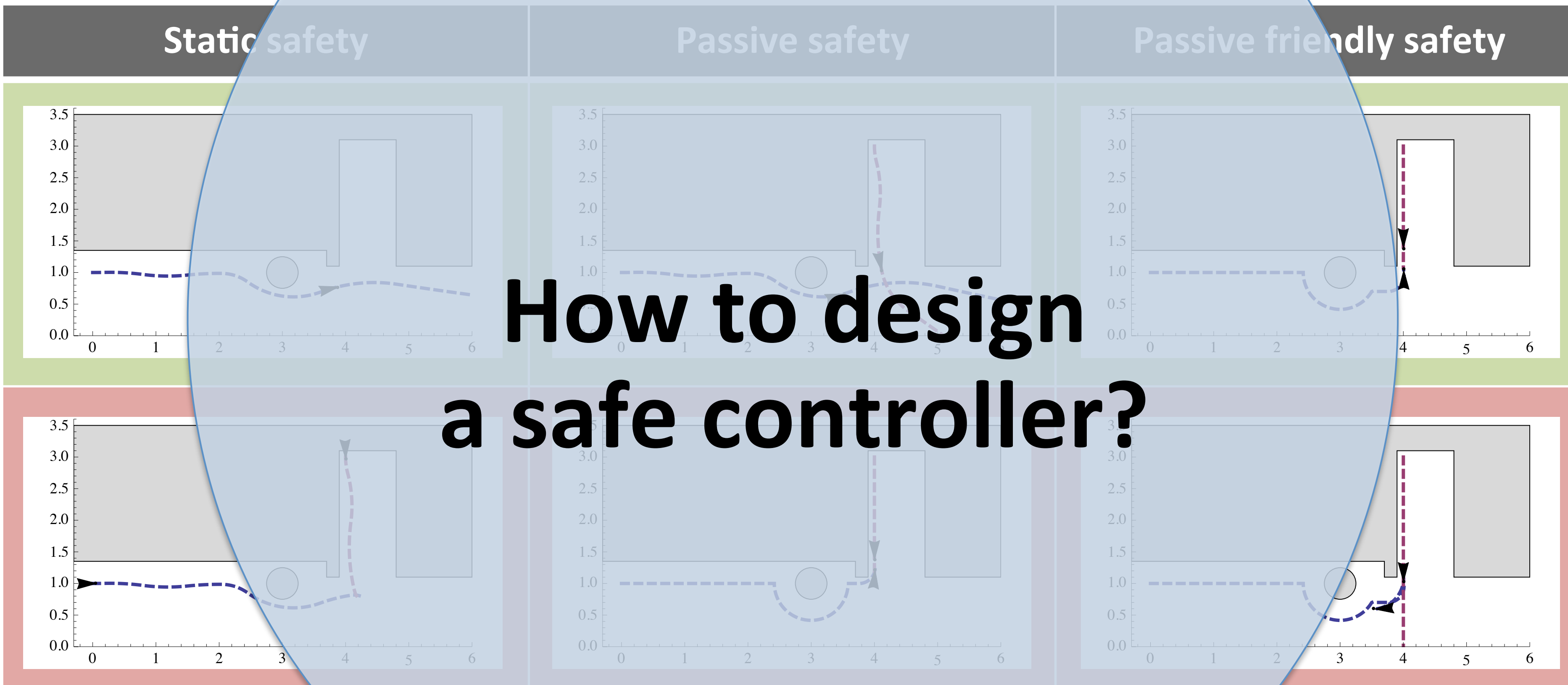
Static safety	Passive safety	Passive friendly safety



.:: Safety Definitions

Static safety	Passive safety	Passive friendly safety
		
		

.:: Safety Definitions



How to design a safe controller?

.:: Constraints of a Safe Controller

Name	Invariant	Switching
Static safety	$\|p_r - p_o\|_\infty > \frac{v_r^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon v_r\right)$	
Passive safety	$v_r = 0 \vee \|p_r - p_o\|_\infty > \frac{v_r^2}{2b} + V\frac{v_r}{b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v_r + V)\right)$	
	Sensor uncertainty $\|\tilde{p}_r - p_o\|_\infty > \frac{v_r^2}{2b} + V\frac{v_r}{b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v_r + V)\right) + U_p$	
	Actuator disturbance $\|p_r - p_o\|_\infty > \frac{v_r^2}{2bU_m} + V\frac{v_r}{bU_m} + \left(\frac{A}{bU_m} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v_r + V)\right)$	
	Sensor failure $\|\tilde{p}_r - p_o\|_\infty > \frac{v_r^2}{2b} + V\frac{v_r}{b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v + V)\right) + U_p + g\Delta$	
Passive friendly safety	$v_r = 0 \vee \|p_r - p_o\|_\infty > \frac{v_r^2}{2b} + \frac{V^2}{2b_o} + V\left(\frac{v_r}{b} + \tau\right) + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v_r + V)\right)$	

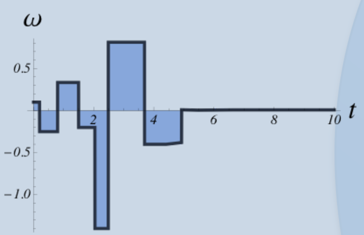
.:: Constraints of a Safe Controller

Name	Invariant	Switching
Static safety		$\|p_r - p_o\|_\infty > \frac{v_r^2}{2b} + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon v_r\right)$
Passive safety		$v_r = 0 \lor \|p_r - p_o\|_\infty > \frac{v_r^2}{2b} + V\frac{v_r}{b} + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v_r + V)\right)$
	Sensor uncertainty	$\|\tilde{p}_r - p_o\|_\infty > \frac{v_r^2}{2b} + V\frac{v_r}{b} + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v_r + V)\right) + U_p$
	Actuator disturbance	$\|p_r - p_o\|_\infty > \frac{v_r^2}{2bU_m} + V\frac{v_r}{bU_m} + \left(\frac{A}{bU_m}+1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v_r + V)\right)$
	Sensor failure	$\|\tilde{p}_r - p_o\|_\infty > \frac{v_r^2}{2b} + V\frac{v_r}{b} + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v + V)\right) + U_p + g\Delta$
Passive friendly safety		$v_r = 0 \lor \|p_r - p_o\|_\infty > \frac{v_r^2}{2b} + \frac{V^2}{2b_o} + V\left(\frac{v_r}{b} + \tau\right) + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v_r + V)\right)$

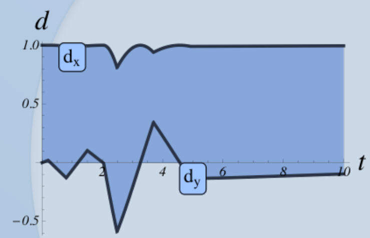
How to find & justify those?

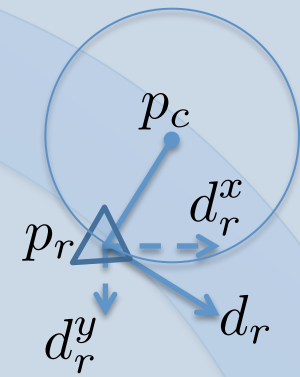
.:: Formal Verification to the Rescue

Control
- Steer
- Accelerate…

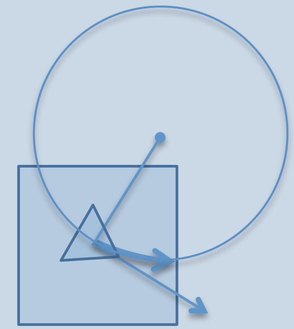


Physics
- Newtonian rigid body dynamics



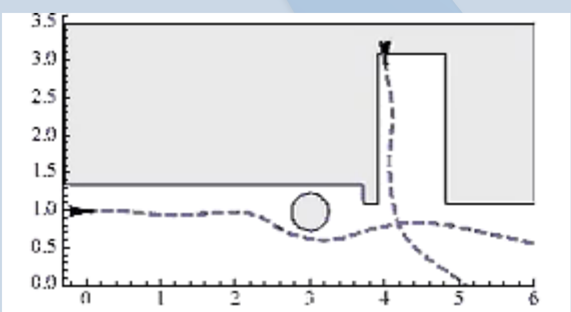


Move on circle

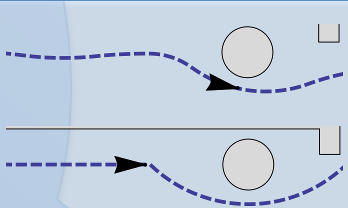


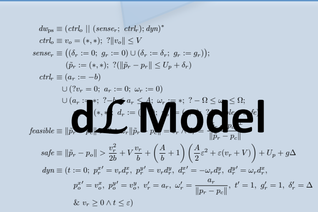
Stay in the box

Hybrid System



Drive Variants
- Differential
- Omnidirectional





d$\mathcal{L}$ Model

.:: Model and Proof

Theorem: $\psi_{ps} \rightarrow [dw_{ps}]\left((v_r = 0) \vee \left(\|p_r - p_o\| > \frac{v_r^2}{2b} + V\frac{v_r}{b}\right)\right)$

Initial Conditions → [Hybrid System] (Requirements)

Passive Safety

$$dw_{\text{ps}} \equiv (ctrl_o \;||\; (sense_r;\; ctrl_r); dyn)^*$$

$$ctrl_o \equiv v_o = (*,*);\; ?\|v_o\| \le V$$

$$sense_r \equiv \big((\delta_r := 0;\; g_r := 0) \cup (\delta_r := \delta_r;\; g_r := g_r)\big);$$
$$(\tilde{p}_r := (*,*);\; ?(\|\tilde{p}_r - p_r\| \le U_p + \delta_r)$$

$$ctrl_r \equiv (a_r := -b)$$
$$\cup\, (?v_r = 0;\; a_r := 0;\; \omega_r := 0)$$
$$\cup\, (a_r := *;\; ?{-b} \le a_r \le A;\; \omega_r := *;\; ? - \Omega \le \omega_r \le \Omega;$$
$$p_c := (*,*);\; d_r := (*,*);\; p_o := (*,*);\; ?feasible \wedge safe)$$

$$feasible \equiv \|\tilde{p}_r - p_c\| > 0 \wedge \omega_r\|\tilde{p}_r - p_c\| = v_r \wedge d_r = \frac{(\tilde{p}_r - p_c)^{\perp}}{\|\tilde{p}_r - p_c\|}$$

$$safe \equiv \|\tilde{p}_r - p_o\| > \frac{v_r^2}{2b} + V\frac{v_r}{b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v_r + V)\right) + U_p + g\Delta$$

$$dyn \equiv (t := 0;\; p_r^{x\prime} = v_r d_r^x,\; p_r^{y\prime} = v_r d_r^y,\; d_r^{x\prime} = -\omega_r d_r^y,\; d_r^{y\prime} = \omega_r d_r^x,$$
$$p_o^{x\prime} = v_o^x,\; p_o^{y\prime} = v_o^y,\; v_r' = a_r,\; \omega_r' = \frac{a_r}{\|p_r - p_c\|},\; t' = 1,\; g_r' = 1,\; \delta_r' = \Delta$$
$$\&\; v_r \ge 0 \wedge t \le \varepsilon)$$

.:: Model and Proof

Theorem: $\psi_{ps} \rightarrow [dw_{ps}]\left((v_r = 0) \vee \left(\|p_r - p_o\| > \frac{v_r^2}{2b} + V\frac{v_r}{b}\right)\right)$

Initial Conditions → [Hybrid System] (Requirements)

$$\begin{aligned}
dw_{\text{ps}} &\equiv (ctrl_o \mid\mid (sense_r;\; ctrl_r);\, dyn)^* \\
ctrl_o &\equiv v_o = (*,*);\; ?\|v_o\| \leq V \\
sense_r &\equiv \big((\delta_r := 0;\; g_r := 0) \cup (\delta_r := \delta_r;\; g_r := g_r)\big); \\
&\quad (\tilde{p}_r := (*,*);\; ?(\|\tilde{p}_r - p_r\| \leq U_p + \delta_r) \\
ctrl_r &\equiv (a_r := -b) \\
&\quad \cup (?v_r = 0;\; a_r := 0;\; \omega_r := 0) \\
&\quad \cup (a_r := *;\; ?{-b} \leq a_r \leq A;\; \omega_r := *;\; ? - \Omega \leq \omega_r \leq \Omega; \\
&\qquad p_c := (*,*);\; d_r := (*,*);\; p_o := (*,*);\; ?feasible \wedge safe) \\
feasible &\equiv \|\tilde{p}_r - p_c\| > 0 \wedge \omega_r\|\tilde{p}_r - p_c\| = v_r \wedge d_r = \frac{(\tilde{p}_r - p_c)^\perp}{\|\tilde{p}_r - p_c\|} \\
safe &\equiv \|\tilde{p}_r - p_o\| > \frac{v_r^2}{2b} + V\frac{v_r}{b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v_r + V)\right) + U_p + g\Delta \\
dyn &\equiv (t := 0;\; p_r^{x\prime} = v_r d_r^x,\; p_r^{y\prime} = v_r d_r^y,\; d_r^{x\prime} = -\omega_r d_r^y,\; d_r^{y\prime} = \omega_r d_r^x, \\
&\qquad p_o^{x\prime} = v_o^x,\; p_o^{y\prime} = v_o^y,\; v_r' = a_r,\; \omega_r' = \frac{a_r}{\|p_r - p_c\|},\; t' = 1,\; g_r' = 1,\; \delta_r' = \Delta \\
&\qquad \&\; v_r \geq 0 \wedge t \leq \varepsilon)
\end{aligned}$$

Obstacle Behavior

.:: Model and Proof

Theorem: $\psi_{ps} \rightarrow [dw_{ps}]\left((v_r = 0) \vee \left(\|p_r - p_o\| > \frac{v_r^2}{2b} + V\frac{v_r}{b}\right)\right)$

Initial Conditions → [Hybrid System] (Requirements)

$$dw_{\text{ps}} \equiv (ctrl_o \;||\; (sense_r;\; ctrl_r); dyn)^*$$

$$ctrl_o \equiv v_o = (*,*);\; ?\|v_o\| \leq V$$

$$sense_r \equiv \big((\delta_r := 0;\; g_r := 0) \cup (\delta_r := \delta_r;\; g_r := g_r)\big);\; (\tilde{p}_r := (*,*);\; ?(\|\tilde{p}_r - p_r\| \leq U_p + \delta_r)$$

Robot Sensing

$$\begin{aligned} ctrl_r \equiv\; & (a_r := -b) \\ & \cup (?v_r = 0;\; a_r := 0;\; \omega_r := 0) \\ & \cup (a_r := *;\; ?{-b} \leq a_r \leq A;\; \omega_r := *;\; ? -\Omega \leq \omega_r \leq \Omega; \\ & \quad p_c := (*,*);\; d_r := (*,*);\; p_o := (*,*);\; ?feasible \wedge safe) \end{aligned}$$

$$feasible \equiv \|\tilde{p}_r - p_c\| > 0 \wedge \omega_r\|\tilde{p}_r - p_c\| = v_r \wedge d_r = \frac{(\tilde{p}_r - p_c)^{\perp}}{\|\tilde{p}_r - p_c\|}$$

$$safe \equiv \|\tilde{p}_r - p_o\| > \frac{v_r^2}{2b} + V\frac{v_r}{b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v_r + V)\right) + U_p + g\Delta$$

$$\begin{aligned} dyn \equiv\; & (t := 0;\; p_r^{x\prime} = v_r d_r^x,\; p_r^{y\prime} = v_r d_r^y,\; d_r^{x\prime} = -\omega_r d_r^y,\; d_r^{y\prime} = \omega_r d_r^x, \\ & p_o^{x\prime} = v_o^x,\; p_o^{y\prime} = v_o^y,\; v_r' = a_r,\; \omega_r' = \frac{a_r}{\|p_r - p_c\|},\; t' = 1,\; g_r' = 1,\; \delta_r' = \Delta \\ & \&\; v_r \geq 0 \wedge t \leq \varepsilon) \end{aligned}$$

.:: Model and Proof

Theorem: $\psi_{ps} \rightarrow [dw_{ps}]\left((v_r = 0) \vee \left(\|p_r - p_o\| > \frac{v_r^2}{2b} + V\frac{v_r}{b}\right)\right)$

Initial Conditions → [Hybrid System] (Requirements)

$$
\begin{aligned}
dw_{\text{ps}} &\equiv (ctrl_o \;||\; (sense_r;\; ctrl_r);\, dyn)^* \\
ctrl_o &\equiv v_o = (*,*);\; ?\|v_o\| \leq V \\
sense_r &\equiv \big((\delta_r := 0;\; g_r := 0) \cup (\delta_r := \delta_r;\; g_r := g_r)\big); \\
&\quad (\tilde{p}_r := (*,*);\; ?(\|\tilde{p}_r - p_r\| \leq U_p + \delta_r) \\
ctrl_r &\equiv (a_r := -b) \\
&\quad \cup (?v_r = 0;\; a_r := 0;\; \omega_r := 0) \\
&\quad \cup (a_r := *;\; ?{-b} \leq a_r \leq A;\; \omega_r := *;\; ? -\Omega \leq \omega_r \leq \Omega; \\
&\qquad p_c := (*,*);\; d_r := (*,*);\; p_o := (*,*);\; ?feasible \wedge safe)
\end{aligned}
$$

Robot Control

$$
\begin{aligned}
feasible &\equiv \|\tilde{p}_r - p_c\| > 0 \wedge \omega_r\|\tilde{p}_r - p_c\| = v_r \wedge d_r = \frac{(\tilde{p}_r - p_c)^\perp}{\|\tilde{p}_r - p_c\|} \\
safe &\equiv \|\tilde{p}_r - p_o\| > \frac{v_r^2}{2b} + V\frac{v_r}{b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v_r + V)\right) + U_p + g\Delta \\
dyn &\equiv (t := 0;\; p_r^{x\prime} = v_r d_r^x,\; p_r^{y\prime} = v_r d_r^y,\; d_r^{x\prime} = -\omega_r d_r^y,\; d_r^{y\prime} = \omega_r d_r^x, \\
&\quad p_o^{x\prime} = v_o^x,\; p_o^{y\prime} = v_o^y,\; v_r' = a_r,\; \omega_r' = \frac{a_r}{\|p_r - p_c\|},\; t' = 1,\; g_r' = 1,\; \delta_r' = \Delta \\
&\quad \&\; v_r \geq 0 \wedge t \leq \varepsilon)
\end{aligned}
$$

.:: Model and Proof

Theorem: $\psi_{ps} \rightarrow [dw_{ps}]\left((v_r = 0) \vee \left(\|p_r - p_o\| > \frac{v_r^2}{2b} + V\frac{v_r}{b}\right)\right)$

Initial Conditions → [Hybrid System] (Requirements)

$$
\begin{aligned}
dw_{\text{ps}} &\equiv (ctrl_o \;||\; (sense_r;\; ctrl_r); dyn)^* \\
ctrl_o &\equiv v_o = (*,*);\; ?\|v_o\| \le V \\
sense_r &\equiv \big((\delta_r := 0;\; g_r := 0) \cup (\delta_r := \delta_r;\; g_r := g_r)\big); \\
&\quad (\tilde{p}_r := (*,*);\; ?(\|\tilde{p}_r - p_r\| \le U_p + \delta_r) \\
ctrl_r &\equiv (a_r := -b) \\
&\quad \cup (?v_r = 0;\; a_r := 0;\; \omega_r := 0) \\
&\quad \cup (a_r := *;\; ?{-b} \le a_r \le A;\; \omega_r := *;\; ? - \Omega \le \omega_r \le \Omega; \\
&\qquad p_c := (*,*);\; d_r := (*,*);\; p_o := (*,*);\; ?feasible \wedge safe)
\end{aligned}
$$

Safe Curve

$$
\begin{aligned}
feasible &\equiv \|\tilde{p}_r - p_c\| > 0 \wedge \omega_r\|\tilde{p}_r - p_c\| = v_r \wedge d_r = \frac{(\tilde{p}_r - p_c)^\perp}{\|\tilde{p}_r - p_c\|} \\
safe &\equiv \|\tilde{p}_r - p_o\| > \frac{v_r^2}{2b} + V\frac{v_r}{b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v_r + V)\right) + U_p + g\Delta
\end{aligned}
$$

$$
\begin{aligned}
dyn &\equiv (t := 0;\; p_r^{x\prime} = v_r d_r^x,\; p_r^{y\prime} = v_r d_r^y,\; d_r^{x\prime} = -\omega_r d_r^y,\; d_r^{y\prime} = \omega_r d_r^x, \\
&\quad p_o^{x\prime} = v_o^x,\; p_o^{y\prime} = v_o^y,\; v_r' = a_r,\; \omega_r' = \frac{a_r}{\|p_r - p_c\|},\; t' = 1,\; g_r' = 1,\; \delta_r' = \Delta \\
&\quad \&\; v_r \ge 0 \wedge t \le \varepsilon)
\end{aligned}
$$

.:: Model and Proof

Theorem: $\psi_{ps} \rightarrow [dw_{ps}]\left((v_r = 0) \vee \left(\|p_r - p_o\| > \frac{v_r^2}{2b} + V\frac{v_r}{b}\right)\right)$

Initial Conditions → [Hybrid System] (Requirements)

$$dw_{\text{ps}} \equiv (ctrl_o \;||\; (sense_r;\; ctrl_r); dyn)^*$$

$$ctrl_o \equiv v_o = (*,*);\; ?\|v_o\| \leq V$$

$$sense_r \equiv \big((\delta_r := 0;\; g_r := 0) \cup (\delta_r := \delta_r;\; g_r := g_r)\big);$$
$$(\tilde{p}_r := (*,*);\; ?(\|\tilde{p}_r - p_r\| \leq U_p + \delta_r)$$

$$ctrl_r \equiv (a_r := -b)$$
$$\cup\, (?v_r = 0;\; a_r := 0;\; \omega_r := 0)$$
$$\cup\, (a_r := *;\; ?{-b} \leq a_r \leq A;\; \omega_r := *;\; ? - \Omega \leq \omega_r \leq \Omega;$$
$$p_c := (*,*);\; d_r := (*,*);\; p_o := (*,*);\; ?feasible \wedge safe)$$

$$feasible \equiv \|\tilde{p}_r - p_c\| > 0 \wedge \omega_r\|\tilde{p}_r - p_c\| = v_r \wedge d_r = \frac{(\tilde{p}_r - p_c)^{\perp}}{\|\tilde{p}_r - p_c\|}$$

$$safe \equiv \|\tilde{p}_r - p_o\| > \frac{v_r^2}{2b} + V\frac{v_r}{b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v_r + V)\right) + U_p + g\Delta$$

$$dyn \equiv (t := 0;\; p_r^{x\prime} = v_r d_r^x,\; p_r^{y\prime} = v_r d_r^y,\; d_r^{x\prime} = -\omega_r d_r^y,\; d_r^{y\prime} = \omega_r d_r^x,$$
$$p_o^{x\prime} = v_o^x,\; p_o^{y\prime} = v_o^y,\; v_r' = a_r,\; \omega_r' = \frac{a_r}{\|p_r - p_c\|},\; t' = 1,\; g_r' = 1,\; \delta_r' = \Delta$$
$$\&\; v_r \geq 0 \wedge t \leq \varepsilon)$$

Continuous Dynamics

.:: Model and Proof

Theorem: $\psi_{ps} \rightarrow [dw_{ps}] \left((v_r = 0) \vee \left(\|p_r - p_o\| > \frac{v_r^2}{2b} + V\frac{v_r}{b} \right) \right)$

Initial Conditions → [Hybrid System] (Requirements)

$dw_{\text{ps}} \equiv (ctrl_o \mid\mid (sense_r;\ ctrl_r);\ dyn)^*$

$ctrl_o \equiv v_o = (*,*);\ ?\|v_o\| \leq V$

$sense_r \equiv ((\delta_r := 0;\ g_r := 0) \cup (\delta_r := \delta_r;\ g_r := g_r));$
$(\tilde{p}_r := (*,*);\ ?(\|\tilde{p}_r - p_r\| \leq U_p + \delta_r)$

$ctrl_r \equiv (a_r := -$ …
$\cup\ (?v_r = 0;\ a_r := 0;\ \omega_r := 0)$
$\cup\ (a_r := *;\ ?{-b} \leq a_r \leq A;\ \omega_r := *;\ ? - \Omega \leq \omega_r \leq \Omega;$
$p_c := (*,*);\ d_r := (*,*);\ p_o := (*,*);\ ?feasible \wedge safe)$

✔ Verified in KeYmaera

- Proof
- Switching constraints
- Design implications & trade-offs

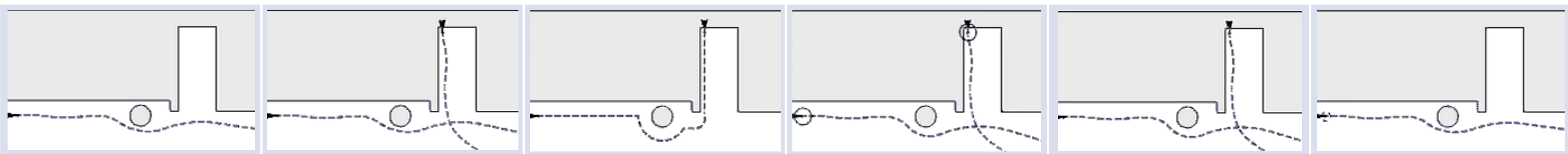
$feasible \equiv \|\tilde{p}_r - p_c\| > 0 \wedge \omega_r\|\tilde{p}_r - p_c\| = v_r \wedge d_r = \frac{(\tilde{p}_r - p_c)^\perp}{\|\tilde{p}_r - p_c\|}$

$safe \equiv \|\tilde{p}_r - p_o\| > \frac{v_r^2}{2b} + V\frac{v_r}{b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v_r + V)\right) + U_p + g\Delta$

$dyn \equiv (t := 0;\ p_r^{x\prime} = v_r d_r^x,\ p_r^{y\prime} = v_r d_r^y,\ d_r^{x\prime} = -\omega_r d_r^y,\ d_r^{y\prime} = \omega_r d_r^x,$
$p_o^{x\prime} = v_o^x,\ p_o^{y\prime} = v_o^y,\ v_r' = a_r,\ \omega_r' = \frac{a_r}{\|p_r - p_c\|},\ t' = 1,\ g_r' = 1,\ \delta_r' = \Delta$
$\&\ v_r \geq 0 \wedge t \leq \varepsilon)$

.:: Provably Safe Obstacle Avoidance

Static safety	Passive safety	Friendly safety	Sensor uncertainty	Actuator disturbance	Sensor failure



Case Studies

Visit us at

symbolaris.com

Tools

Sφnx **KeYmaera**