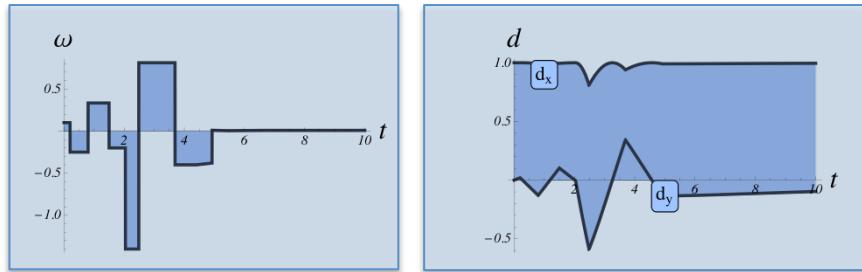
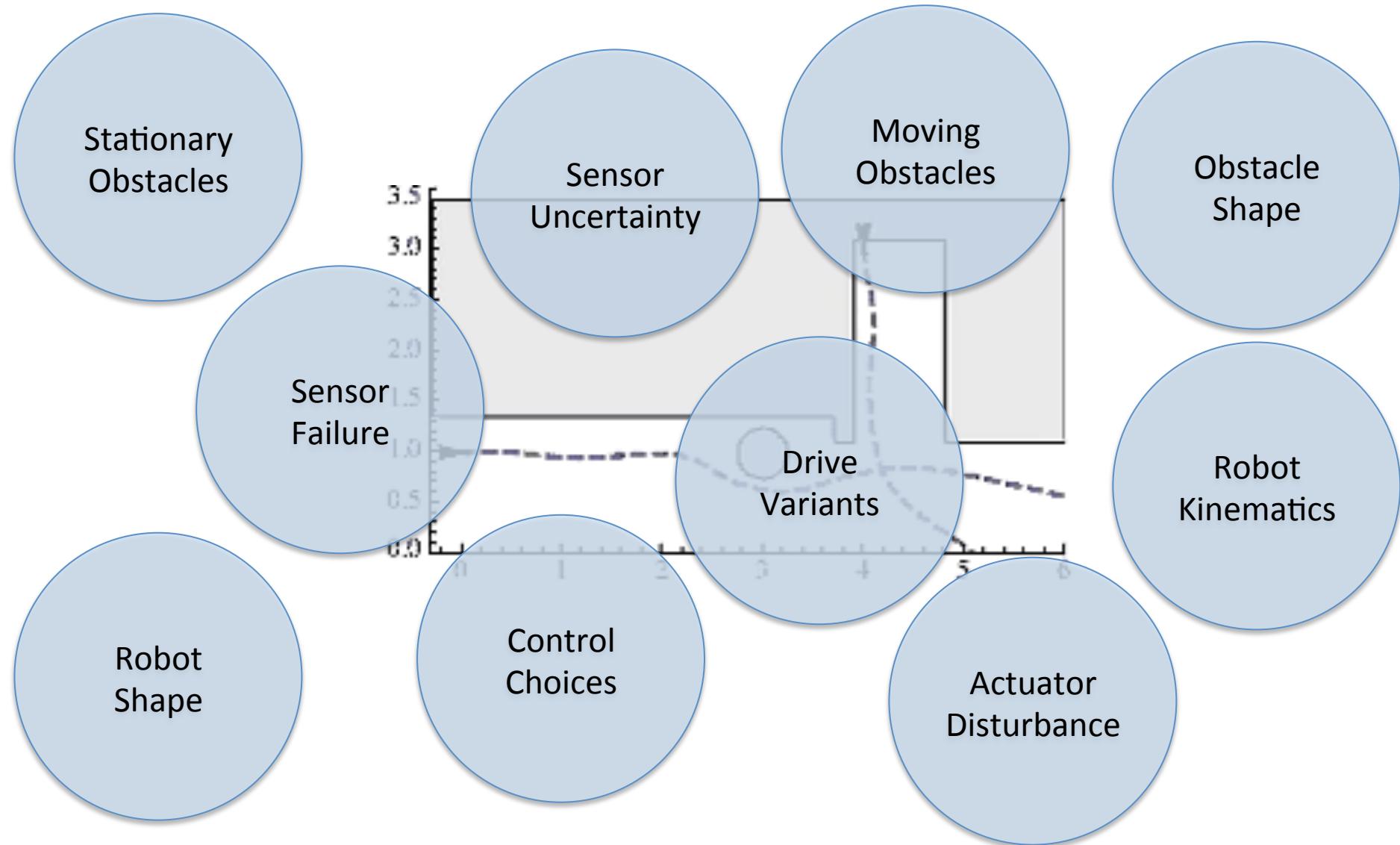


# Safe Obstacle Avoidance of Autonomous Robotic Ground Vehicles



**Stefan Mitsch, Khalil Ghorbal and André Platzer**  
Computer Science Department  
Carnegie Mellon University

# ... Obstacle Avoidance



# ... Obstacle Avoidance

**How can we build a  
robot that is safe?**

Stationary  
Obstacles

Sensor  
Uncertainty

Moving  
Obstacles

Obstacle  
Shape

Robot  
Shape

Control  
Choices

Actuator  
Disturbance

Sensor  
Failure

Variants

Robot  
Kinematics

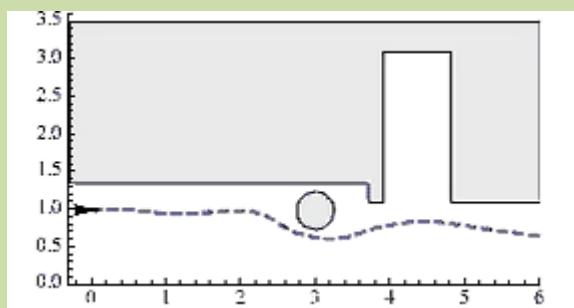
# ... Obstacle Avoidance

**What is safe?**

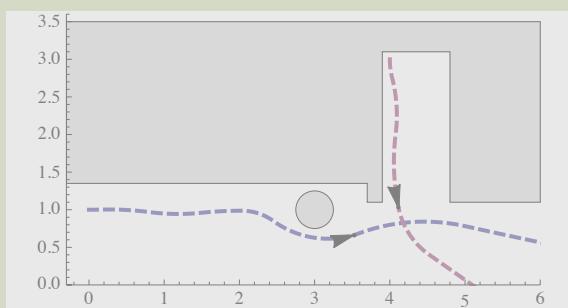


# ... Safety Definitions

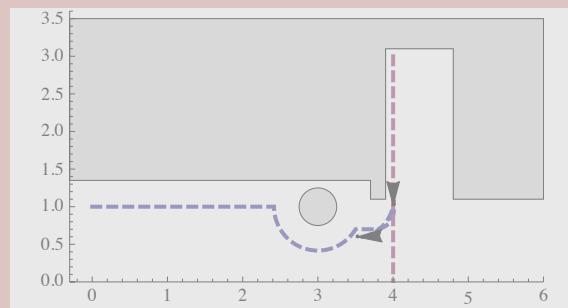
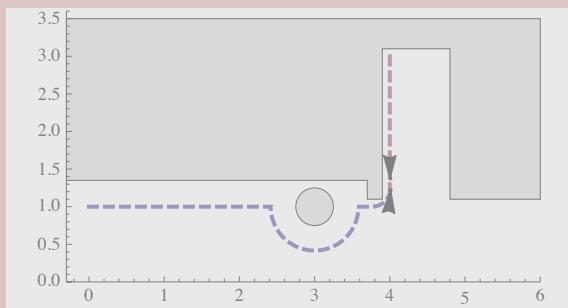
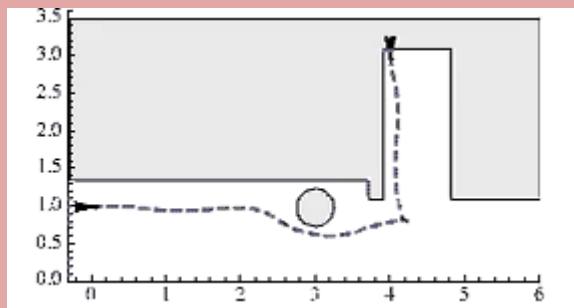
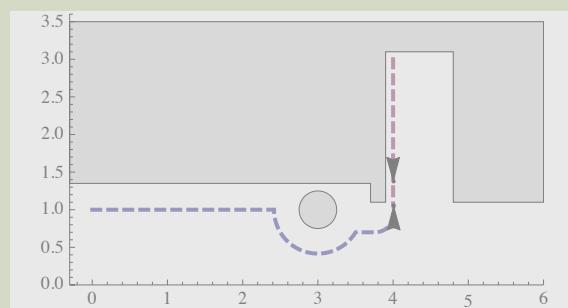
Static safety



Passive safety

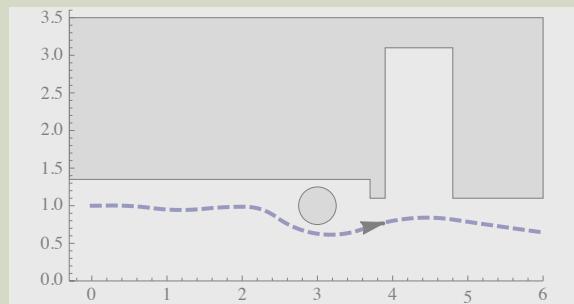


Passive friendly safety

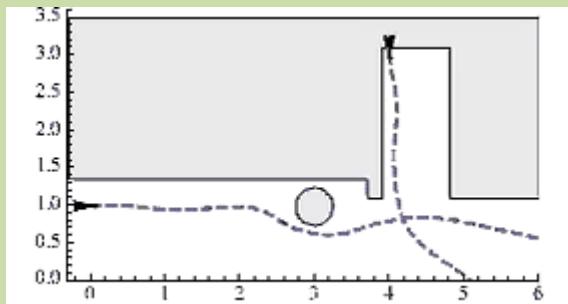


# ... Safety Definitions

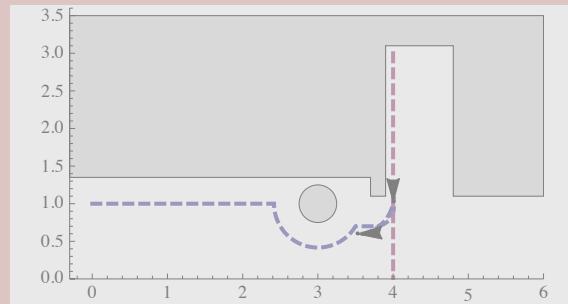
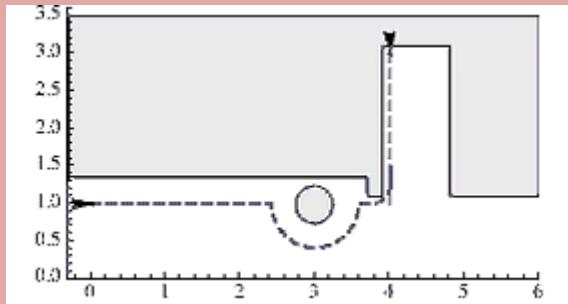
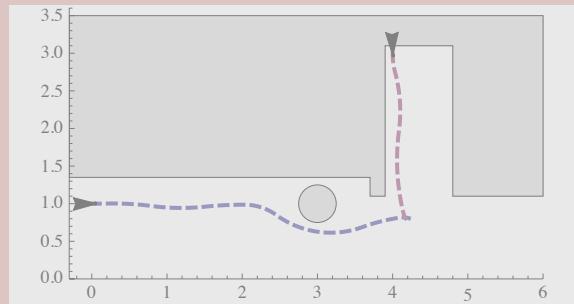
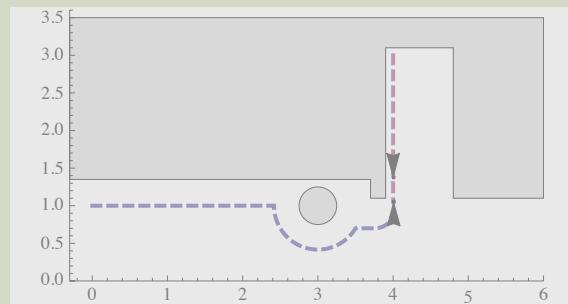
Static safety



Passive safety

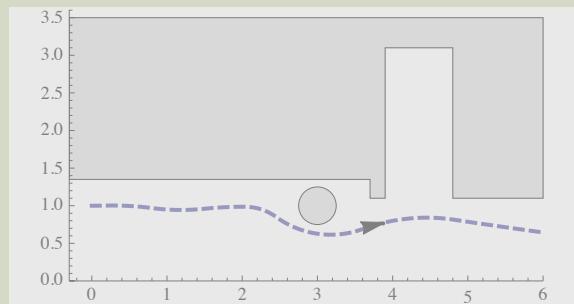


Passive friendly safety

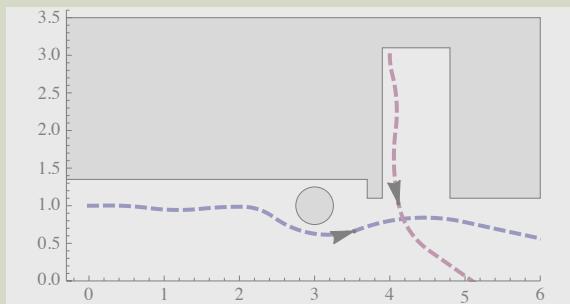


# ... Safety Definitions

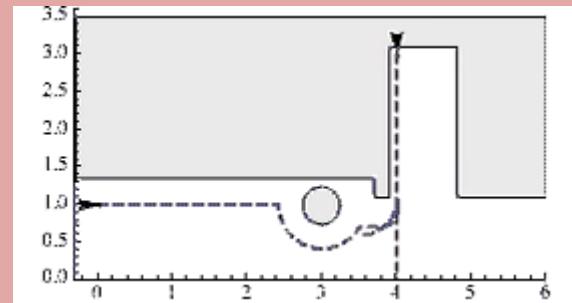
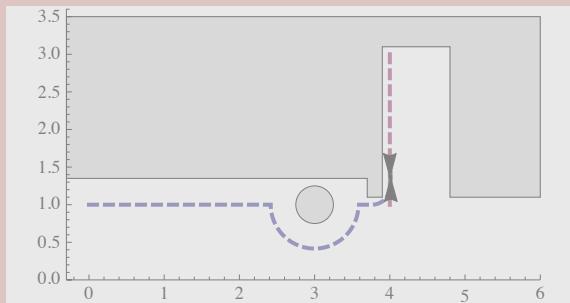
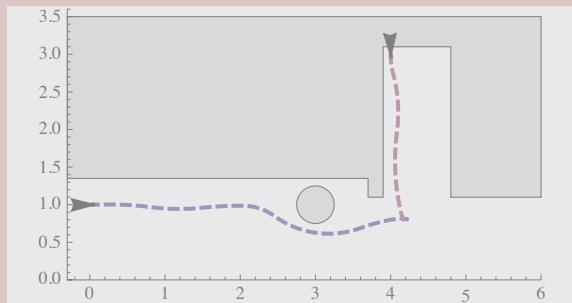
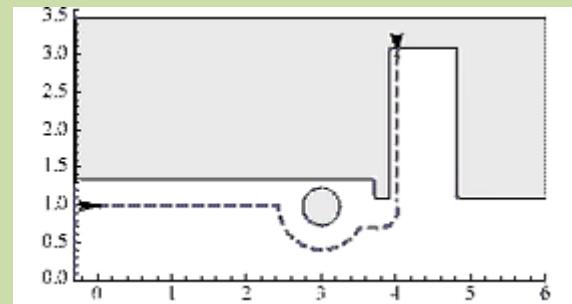
Static safety



Passive safety

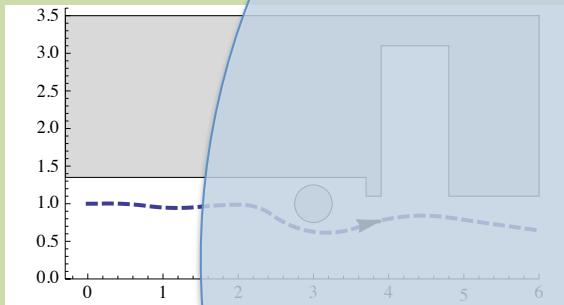


Passive friendly safety



# ... Safety Definitions

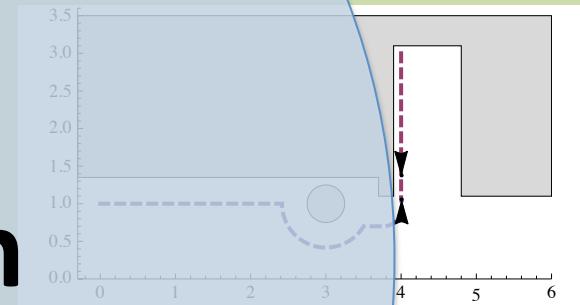
Static safety



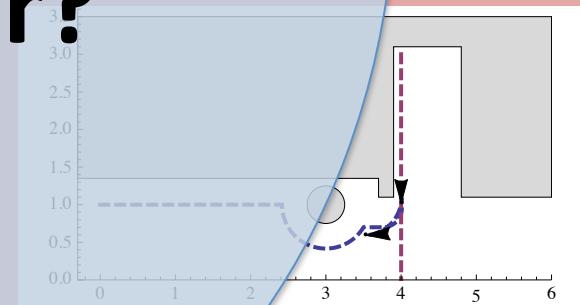
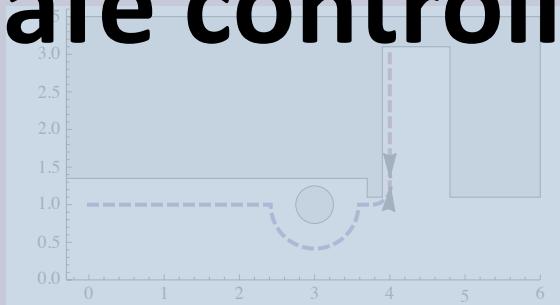
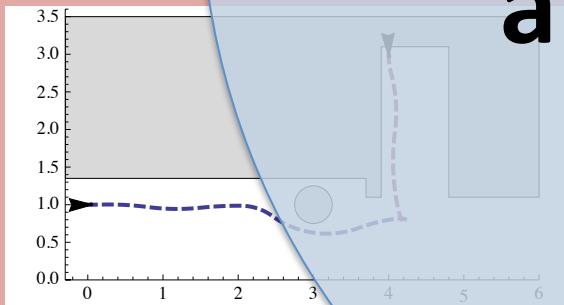
Passive safety



Passive friendly safety



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

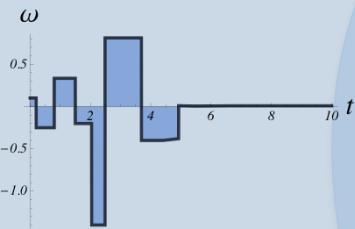
**How to find & justify those?**

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		$\ \tilde{p}_r - p_o\ _\infty > \frac{v_r^2}{2b} + V \frac{v_r}{b} + \left(\frac{A}{b} + 1\right) \left(\frac{A}{2}\varepsilon^2 + \varepsilon(v_r + V)\right) + U_p + g\Delta$
Passive friendly safety		$v_r = 0 \vee \ p_r - p_o\ _\infty > \frac{v_r^2}{2b} + \frac{V^2}{2b_o} + V \left(\frac{v_r}{b} + \tau\right) + \left(\frac{A}{b} + 1\right) \left(\frac{A}{2}\varepsilon^2 + \varepsilon(v_r + V)\right)$

# ... Formal Verification to the Rescue

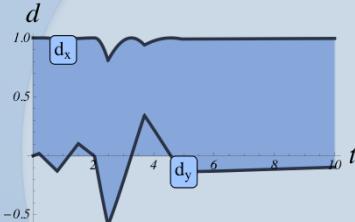
## Control

- Steer
- Accelerate...

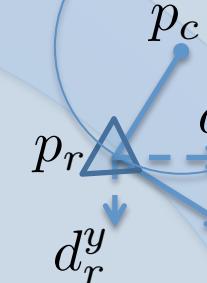
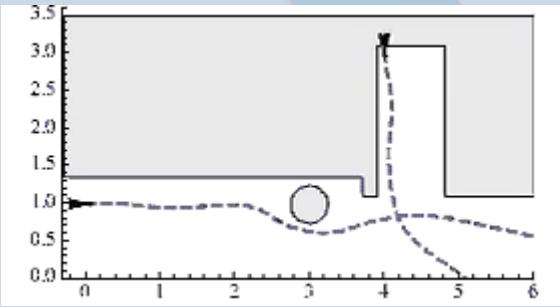


## Physics

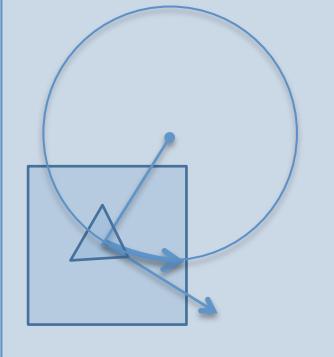
- Newtonian rigid body dynamics



## Hybrid System



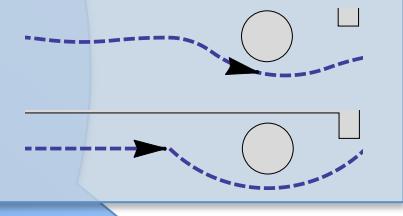
**Move on circle**



**Stay in the box**

## Drive Variants

- Differential
- Omnidirectional



**dL Model**

$$\begin{aligned} \text{drive} &\equiv (\text{ctrl}_k \mid\mid (\text{sense}_k; \text{ctrl}_k); \text{dyn})^* \\ \text{ctrl}_k &\equiv v_a = (\star, \star); \exists \|v_a\| \leq V \\ \text{sense}_k &\equiv ((d_s := 0; g_s := 0) \cup (d_s := \delta_s; g_s := g_s)); \\ &\quad (\bar{p}_k := (\star, \star); \exists \|\bar{p}_k - p_k\| \leq U_p + \delta_p) \\ \text{ctrl}_k' &\equiv (a_k := -b_k \\ &\quad \cup (v_k := 0; a_k := 0; \omega_k := 0) \\ &\quad \cup (v_k := \gamma_k; a_k := -1; \omega_k := \star; ? - \Omega \leq \omega_k \leq \Omega; \\ &\quad \quad \cup (v_k := \gamma_k; a_k := 1; \omega_k := \star; ? - \Omega \leq \omega_k \leq \Omega; \\ \text{feasible} &\equiv \left[ \frac{\|p_k - \bar{p}_k\|}{\|\bar{p}_k - p_k\|} \right] \leq \frac{\left( \frac{\Delta}{\gamma_k} \right)^2 + \varepsilon(v_k + V)}{\|\bar{p}_k - p_k\|} \end{aligned}$$
$$\begin{aligned} \text{safe} &\equiv \|(p_k - \bar{p}_k)\| > \frac{\Delta}{\gamma_k} + \left( \frac{\Delta}{\gamma_k} + 1 \right) \left( \frac{\Delta}{\gamma_k} \varepsilon^2 + \varepsilon(v_k + V) \right) + U_p + \mu \Delta \\ \text{dyn} &\equiv (t := 0; p_k^0 := v_k d_k^0; p_k^1 := v_k d_k^1; d_k^0 := -\omega_k d_k^0; d_k^1 := \omega_k d_k^1; \\ &\quad p_k^2 := v_k^2; p_k^3 := v_k^3; v_k' := a_k; \omega_k' := \frac{a_k}{\|\bar{p}_k - p_k\|}; \ell' = 1; g_k' = 1; d_k' = \Delta \\ &\quad \& v_k \geq 0 \wedge t \leq \varepsilon) \end{aligned}$$

# ∴ 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)

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

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

$$sense_r \equiv ((\delta_r := 0; g_r := 0) \cup (\delta_r := \delta_r; g_r := g_r));$$

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

$$ctrl_r \equiv (a_r := -b)$$

$$\cup (?v_r = 0; a_r := 0; \omega_r := 0)$$

$$\cup (a_r := *; ?-b \leq a_r \leq A; \omega_r := *; ?-\Omega \leq \omega_r \leq \Omega;$$

$$p_c := (*, *); d_r := (*, *); p_o := (*, *); ?feasible \wedge safe)$$

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

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

$$dyn \equiv (t := 0; p_r^{x'} = v_r d_r^x, p_r^{y'} = v_r d_r^y, d_r^{x'} = -\omega_r d_r^y, d_r^{y'} = \omega_r d_r^x,$$

$$p_o^{x'} = v_o^x, p_o^{y'} = v_o^y, v_r' = a_r, \omega_r' = \frac{a_r}{\|p_r - p_c\|}, t' = 1, g_r' = 1, \delta_r' = \Delta$$

$$\& v_r \geq 0 \wedge t \leq \varepsilon)$$

Passive Safety

# ∴ 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)

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

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

$$sense_r \equiv ((\delta_r := 0; g_r := 0) \cup (\delta_r := \delta_r; g_r := g_r));$$

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

$$ctrl_r \equiv (a_r := -b)$$

$$\cup (?v_r = 0; a_r := 0; \omega_r := 0)$$

$$\cup (a_r := *; ?-b \leq a_r \leq A; \omega_r := *; ?-\Omega \leq \omega_r \leq \Omega;$$

$$p_c := (*, *); d_r := (*, *); p_o := (*, *); ?feasible \wedge safe)$$

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

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

$$dyn \equiv (t := 0; p_r^{x'} = v_r d_r^x, p_r^{y'} = v_r d_r^y, d_r^{x'} = -\omega_r d_r^y, d_r^{y'} = \omega_r d_r^x,$$

$$p_o^{x'} = v_o^x, p_o^{y'} = v_o^y, v_r' = a_r, \omega_r' = \frac{a_r}{\|p_r - p_c\|}, t' = 1, g_r' = 1, \delta_r' = \Delta$$

$$\& v_r \geq 0 \wedge t \leq \varepsilon)$$

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)

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

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

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

Robot Sensing

$$ctrl_r \equiv (a_r := -b)$$

$$\cup (?v_r = 0; a_r := 0; \omega_r := 0)$$

$$\cup (a_r := *; ?-b \leq a_r \leq A; \omega_r := *; ?-\Omega \leq \omega_r \leq \Omega;$$

$$p_c := (*, *); d_r := (*, *); p_o := (*, *); ?feasible \wedge safe)$$

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

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

$$dyn \equiv (t := 0; p_r^{x'} = v_r d_r^x, p_r^{y'} = v_r d_r^y, d_r^{x'} = -\omega_r d_r^y, d_r^{y'} = \omega_r d_r^x,$$

$$p_o^{x'} = v_o^x, p_o^{y'} = v_o^y, v_r' = a_r, \omega_r' = \frac{a_r}{\|p_r - p_c\|}, t' = 1, g_r' = 1, \delta_r' = \Delta$$

$$\& v_r \geq 0 \wedge t \leq \varepsilon)$$

# ∴ 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)

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

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

$$sense_r \equiv ((\delta_r := 0; g_r := 0) \cup (\delta_r := \delta_r; g_r := g_r));$$

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

$$ctrl_r \equiv (a_r := -b)$$

$$\cup (?v_r = 0; a_r := 0; \omega_r := 0)$$

$$\cup (a_r := *; ?-b \leq a_r \leq A; \omega_r := *; ?-\Omega \leq \omega_r \leq \Omega;$$

$$p_c := (*, *); d_r := (*, *); p_o := (*, *); ?feasible \wedge safe)$$

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

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

$$dyn \equiv (t := 0; p_r^{x'} = v_r d_r^x, p_r^{y'} = v_r d_r^y, d_r^{x'} = -\omega_r d_r^y, d_r^{y'} = \omega_r d_r^x,$$

$$p_o^{x'} = v_o^x, p_o^{y'} = v_o^y, v_r' = a_r, \omega_r' = \frac{a_r}{\|p_r - p_c\|}, t' = 1, g_r' = 1, \delta_r' = \Delta$$

$$\& v_r \geq 0 \wedge t \leq \varepsilon)$$

Robot Control

# ∴ 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)

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

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

$$sense_r \equiv ((\delta_r := 0; g_r := 0) \cup (\delta_r := \delta_r; g_r := g_r));$$

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

$$ctrl_r \equiv (a_r := -b)$$

$$\cup (?v_r = 0; a_r := 0; \omega_r := 0)$$

$$\cup (a_r := *; ?-b \leq a_r \leq A; \omega_r := *; ?-\Omega \leq \omega_r \leq \Omega;$$

$$p_c := (*, *); d_r := (*, *); p_o := (*, *); ?feasible \wedge safe$$

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

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

$$dyn \equiv (t := 0; p_r^{x'} = v_r d_r^x, p_r^{y'} = v_r d_r^y, d_r^{x'} = -\omega_r d_r^y, d_r^{y'} = \omega_r d_r^x,$$

$$p_o^{x'} = v_o^x, p_o^{y'} = v_o^y, v_r' = a_r, \omega_r' = \frac{a_r}{\|p_r - p_c\|}, t' = 1, g_r' = 1, \delta_r' = \Delta$$

$$\& v_r \geq 0 \wedge t \leq \varepsilon)$$

Safe Curve

# ∴ 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)

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

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

$$sense_r \equiv ((\delta_r := 0; g_r := 0) \cup (\delta_r := \delta_r; g_r := g_r));$$

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

$$ctrl_r \equiv (a_r := -b)$$

$$\cup (?v_r = 0; a_r := 0; \omega_r := 0)$$

$$\cup (a_r := *; ?-b \leq a_r \leq A; \omega_r := *; ?-\Omega \leq \omega_r \leq \Omega;$$

$$p_c := (*, *); d_r := (*, *); p_o := (*, *); ?feasible \wedge safe)$$

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

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

$$dyn \equiv (t := 0; p_r^{x'} = v_r d_r^x, p_r^{y'} = v_r d_r^y, d_r^{x'} = -\omega_r d_r^y, d_r^{y'} = \omega_r d_r^x,$$

$$p_o^{x'} = v_o^x, p_o^{y'} = v_o^y, v_r' = a_r, \omega_r' = \frac{a_r}{\|p_r - p_c\|}, t' = 1, g_r' = 1, \delta_r' = \Delta$$

$$\& v_r \geq 0 \wedge t \leq \varepsilon)$$

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  $\rightarrow$  [Hybrid System] (Requirements)

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

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

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

$$\begin{aligned} ctrl_r \equiv & (a_r := - \\ & \cup (?v_r = 0; a_r := 0; \omega_r := 0) \end{aligned}$$

$$\cup (a_r := *; ?-b \leq a_r \leq A; \omega_r := -; ?-\Omega \leq \omega_r \leq \Omega;$$

$$p_c := (*, *); d_r := (*, *); p_o := (*, *); ?\text{feasible} \wedge \text{safe})$$

- **Switching constraints**

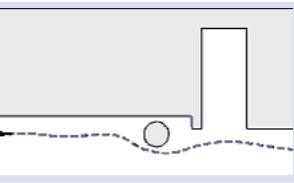
$$\begin{aligned} feasible \equiv & \|\tilde{p}_r - p_c\| > 0 \wedge \omega_r \|\tilde{p}_r - p_c\| = v_r \wedge d_r = \frac{(p_r - p_c)}{\|\tilde{p}_r - p_c\|} \\ & - \quad \text{Design implications \& trade-offs} \end{aligned}$$

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

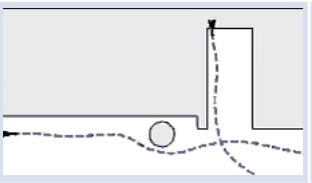
$$\begin{aligned} dyn \equiv & (t := 0; p_r^{x'} = v_r d_r^x, p_r^{y'} = v_r d_r^y, d_r^{x'} = -\omega_r d_r^y, d_r^{y'} = \omega_r d_r^x, \\ & p_o^{x'} = v_o^x, p_o^{y'} = v_o^y, v_r' = a_r, \omega_r' = \frac{a_r}{\|p_r - p_c\|}, t' = 1, g_r' = 1, \delta_r' = \Delta \\ & \wedge v_r \geq 0 \wedge t \leq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

# ... Provable Safety Obstacle Avoidance

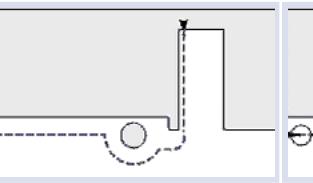
Static safety



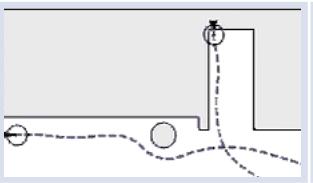
Passive safety



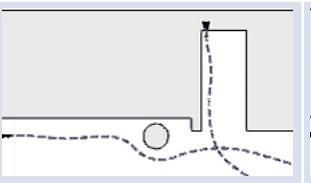
Friendly safety



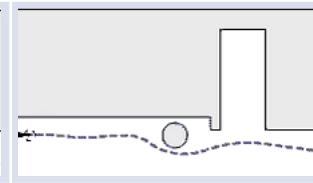
Sensor uncertainty



Actuator disturbance



Sensor failure

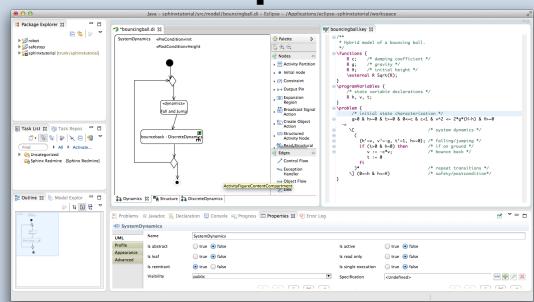


Case Studies

Visit us at  
**symbolaris.com**

Tools

**Sφnx**



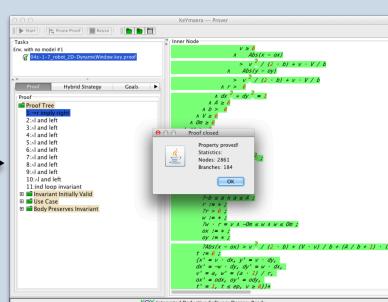
**dL Model**

```

dL = (ctrlL || (senseL; ctrlL); dyn)
ctrlL = v_x = (v_x, *); ?[v_x] ≤ V
senseL = ((delta_x := 0; p_x := 0) ∪ (delta_x := delta_x; p_x := p_x));
    (p_x := (*, *); ?[|p_x - p_x| ≤ U_p + delta_x])
ctrlL = (a_x := -b)
U(a_x = 0; a_x = b; omega_x := 0)
U(v_x = 0; a_x = b; omega_x := 0)
U((v_x = 0; a_x = b; omega_x := 0) & (delta_x = 0; p_x = 0))
    & falling(p_x >= U_p + delta_x)
    & falling(delta_x >= 0)
    & falling(omega_x >= 0)
    & falling(delta_x <= U_p + delta_x)
    & falling(omega_x <= 0)
repeat transitions
    & falling(delta_x <= U_p + delta_x)
    & falling(omega_x <= 0)
end repeat
safe = |p_x - p_x| ≥ U_p + delta_x
dyn = (t := 0; p_x^t := v_x; p_y^t := v_y; d_x^t := -omega_x; d_y^t := -omega_y;
    p_x^{t+1} := v_x; p_y^{t+1} := v_y; d_x^{t+1} := -omega_x; d_y^{t+1} := -omega_y;
    t' = t + 1; g_x = 1; g_y = 1; delta_x = Delta;
    & v_x ≥ 0 & t ≤ c)

```

**KeYmaera**



**Proof**

```

dL = (ctrlL || (senseL; ctrlL); dyn)
ctrlL = v_x = (v_x, *); ?[v_x] ≤ V
senseL = ((delta_x := 0; p_x := 0) ∪ (delta_x := delta_x; p_x := p_x));
    (p_x := (*, *); ?[|p_x - p_x| ≤ U_p + delta_x])
ctrlL = (a_x := -b)
U(a_x = 0; a_x = b; omega_x := 0)
U(v_x = 0; a_x = b; omega_x := 0)
U((a_x := -b) & (v_x = 0) & (delta_x = 0) & (p_x = 0))
    & falling(p_x >= U_p + delta_x)
    & falling(delta_x >= 0)
    & falling(omega_x >= 0)
    & falling(delta_x <= U_p + delta_x)
    & falling(omega_x <= 0)
repeat transitions
    & falling(delta_x <= U_p + delta_x)
    & falling(omega_x <= 0)
end repeat
safe = |p_x - p_x| ≥ U_p + delta_x
dyn = (t := 0; p_x^t := v_x; p_y^t := v_y; d_x^t := -omega_x; d_y^t := -omega_y;
    p_x^{t+1} := v_x; p_y^{t+1} := v_y; d_x^{t+1} := -omega_x; d_y^{t+1} := -omega_y;
    t' = t + 1; g_x = 1; g_y = 1; delta_x = Delta;
    & v_x ≥ 0 & t ≤ c)

```

