# Formal Methods will not Prevent Self-Driving Cars from Having Accidents

*Thierry Fraichard*
*INRIA, LIG-CNRS and Grenoble University*

Forum Méthodes Formelles

Mardi 10 octobre 2017

Embedded France
L'embarqué made in France

informatics mathematics
UNIVERSITÉ Grenoble Alpes

# From Mobile Robots to Self-Driving Cars


Shakey *[66-72]*

Darpa Urban Challenge *[Nov. 07]*

# Why Self-Driving Cars?

Google Official Blog: **What we're driving at**, S. Thrun, 9 October 2010

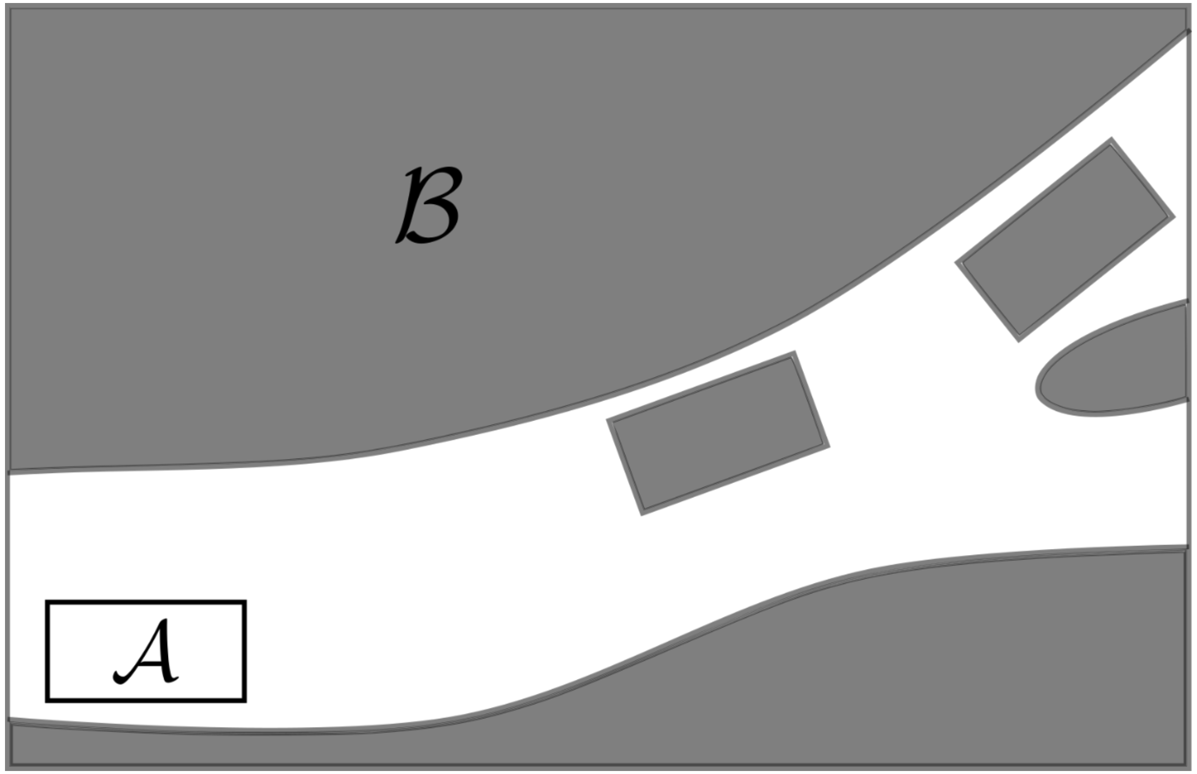
*"Larry and Sergey founded Google because they wanted to help solve really big problems using technology. And one of the big problems we're working on today is car safety and efficiency. Our goal is to help prevent traffic accidents, free up people's time and reduce carbon emissions by fundamentally changing car use.*

*…*

*Safety has been our first priority in this project…"*

2014: 1.25 million deaths worldwide (94% human errors in the US)

# “Absolute” Motion Safety for Self-Driving Cars

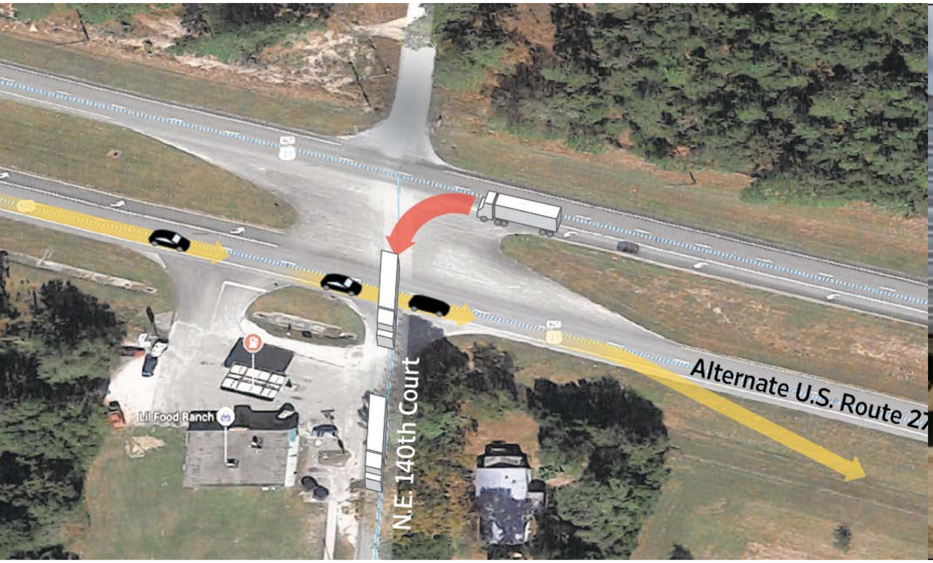



Self-driving car $\mathcal{A}$, roadway “objects” $\mathcal{B}$: $\forall t \in [0, \infty], \mathcal{A}(t) \cap \mathcal{B}(t) = \emptyset$

# Self-Driving Cars and Accidents



# A Fatal Misunderstanding




Tesla Model S crash in “Autopilot” mode, May 2016

The sensors failed to differentiate the white side of the tractor trailer against a brightly lit sky…

# A Harmless Misreasoning


[Google Self-Driving Car Project Monthly Report, February 2016]

*"Our car had detected the approaching bus, but predicted that it would yield to us because we were ahead of it."*

# Why Collisions Happen?

- Hardware failures
- Software bugs
- Misunderstanding
- Misreasoning

- Focus on misreasoning in dynamic environments
- Can motion safety be guaranteed?

# Outline of the Talk

1. **Case study**

   Gaining insight into motion safety

2. **Inevitable collision states**

   **F**urthering the analysis in a formal framework

3. **Motion safety in the real world**

   Houston, we have a problem

4. **Weaker motion safety levels**

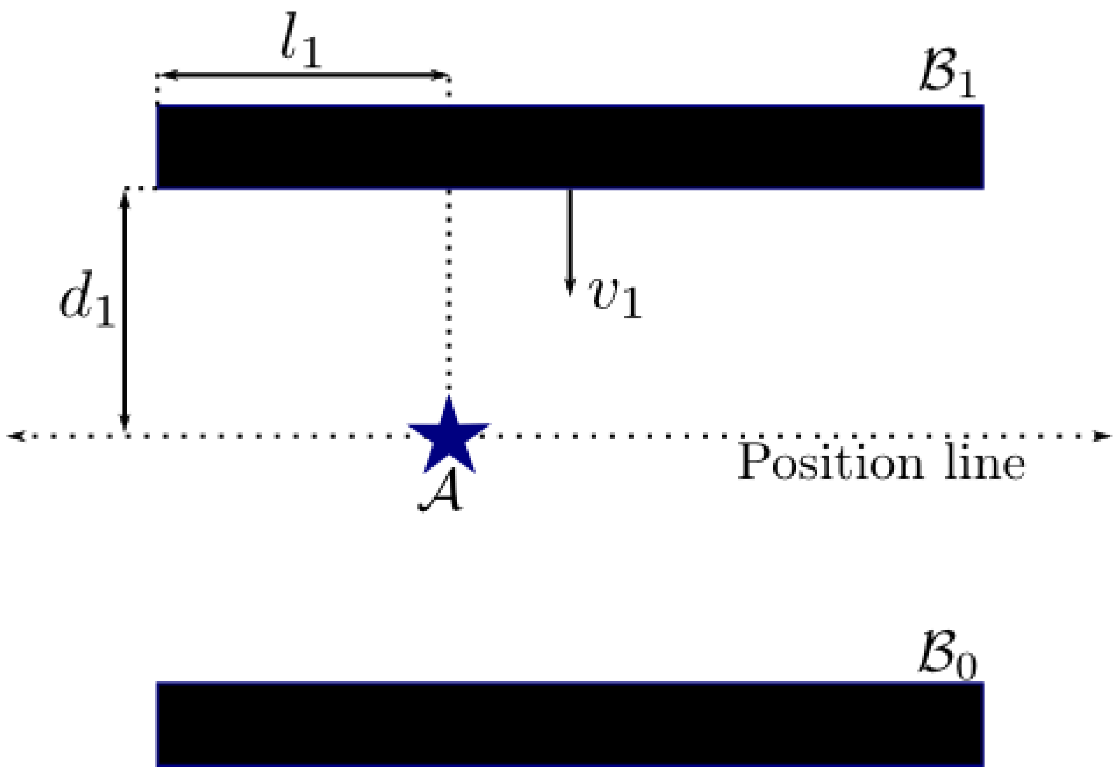
   Less is better than nothing

# 1

## Case Study

*Gaining insight into motion safety*

# The "Compactor" Scenario




$$\mathcal{A} : \dot{p} = v, |v| \leq v_{\max}$$

- Reasoning about the future
  - ✓Collision time
  $$t_c = d_1/v_1$$
  - ✓Escape time
  $$\delta_e = l_1/v_{\max}$$
- Limited decision time
$$\delta_d < t_c - \delta_e$$
- Appropriate time horizon
$$\delta_h > \delta_d + \delta_e$$

# 2

# Inevitable Collision States

*Furthering the analysis in a formal framework*

# Inevitable Collision States *[Fraichard 03]*

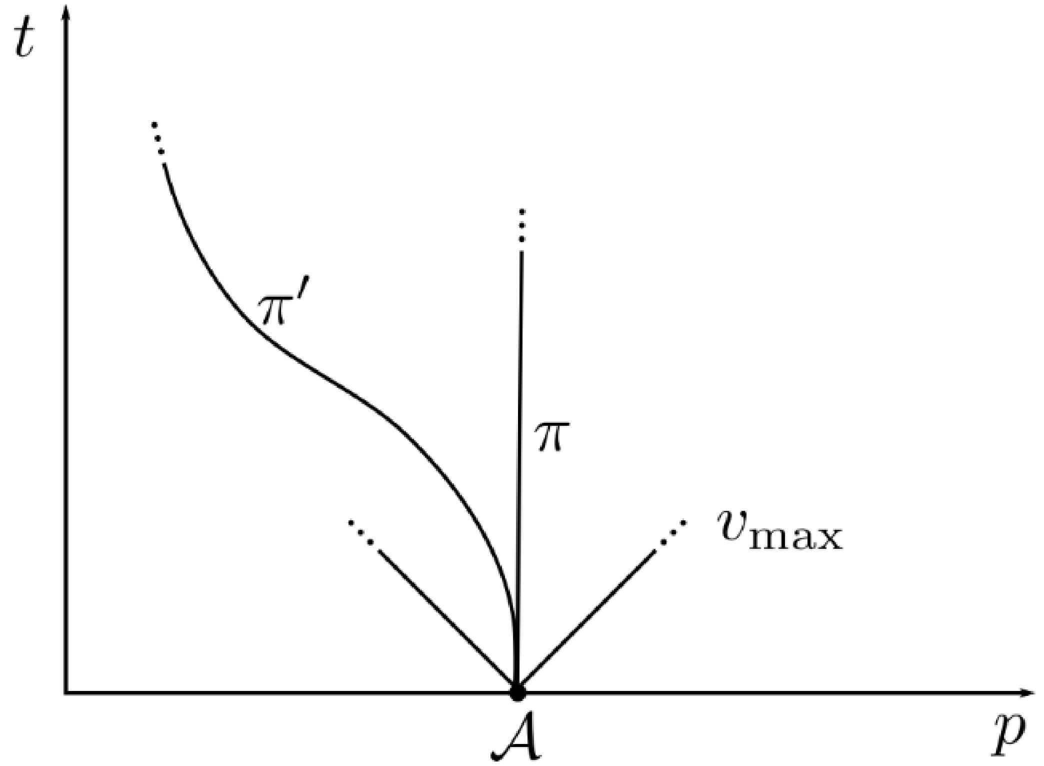
- Collision States (CS) vs. Inevitable Collision States (ICS):
  *Whatever the future trajectory of the robot, a collision will happen*

$\mathcal{A}$: state $s \in \mathcal{S}$, control $u \in \mathcal{U}$, trajectory: $\pi : [t_0, \infty] \longrightarrow \mathcal{U}$
State $s_0$ is:

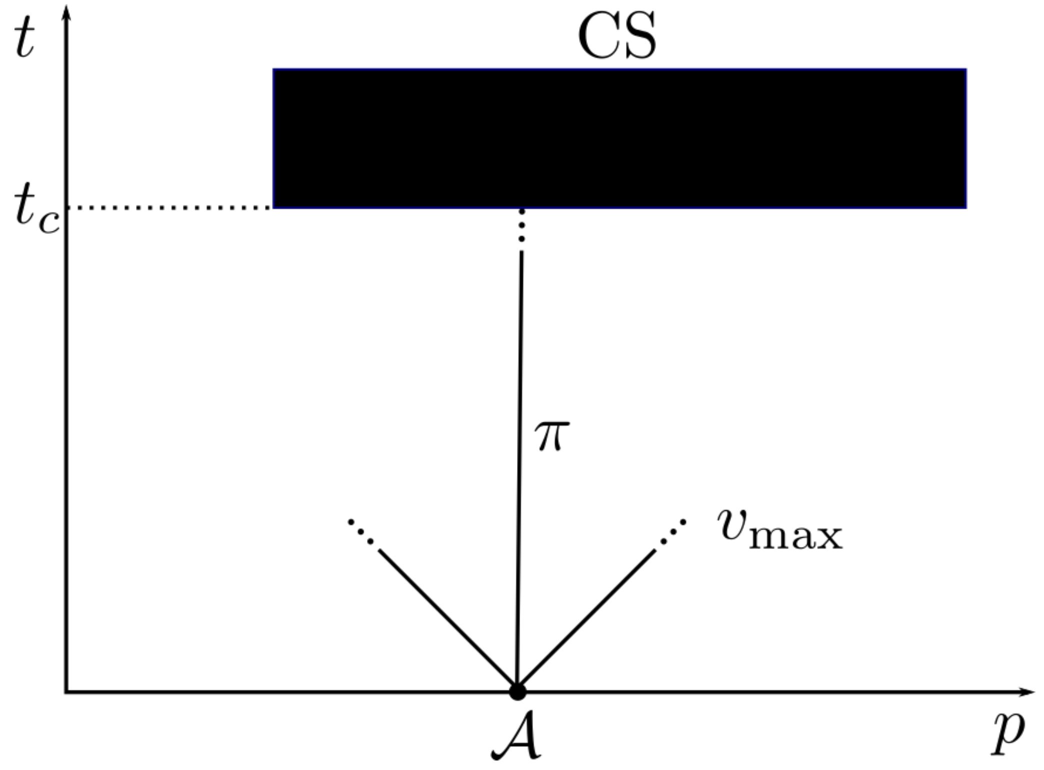
$$\begin{aligned} \text{CS}: &\quad \mathcal{A}(s_0(t)) \cap \mathcal{B}(t) \neq \emptyset \\ \text{ICS}: &\quad \forall \pi, \exists t \in [0, \infty], s(s_0, \pi, t) \in CS \\ \text{(Absolutely) Safe}: &\quad \exists \pi, \forall t \in [0, \infty], s(s_0, \pi, t) \notin CS \end{aligned}$$

- Key to motion safety: **stay away from ICS**

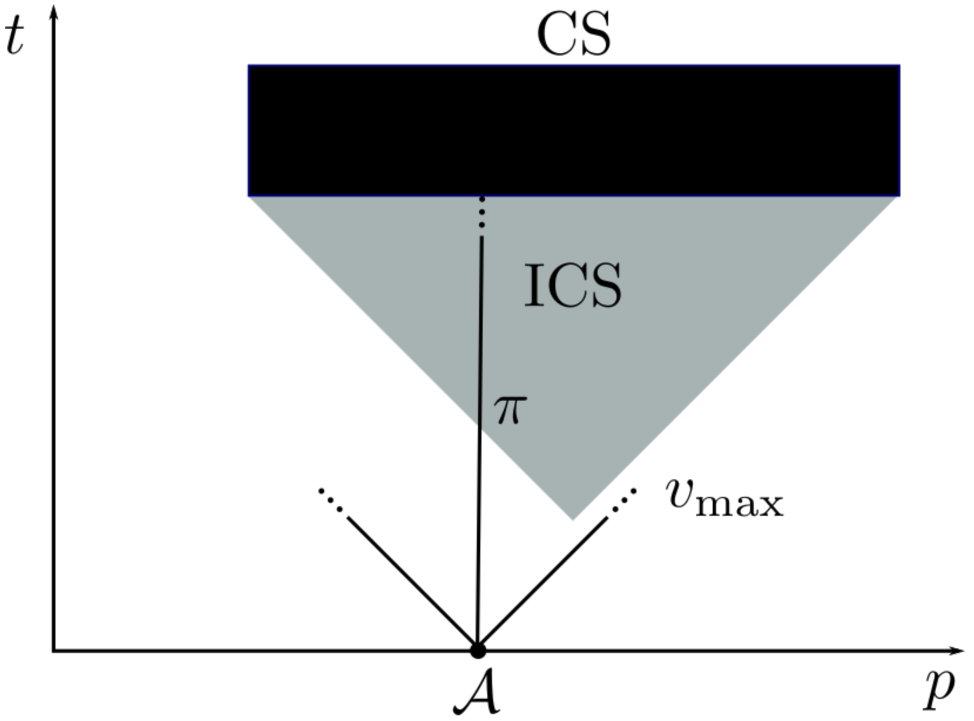
# From Cartesian Space to State-Time Space



# Collision States



# Inevitable Collision States



# Inevitable Collision States' Teachings

1. Obstacles are not independent

   $ICS(\bigcup_i \mathcal{B}_i) \supseteq \bigcup_i ICS(\mathcal{B}_i)$

2. Decision time

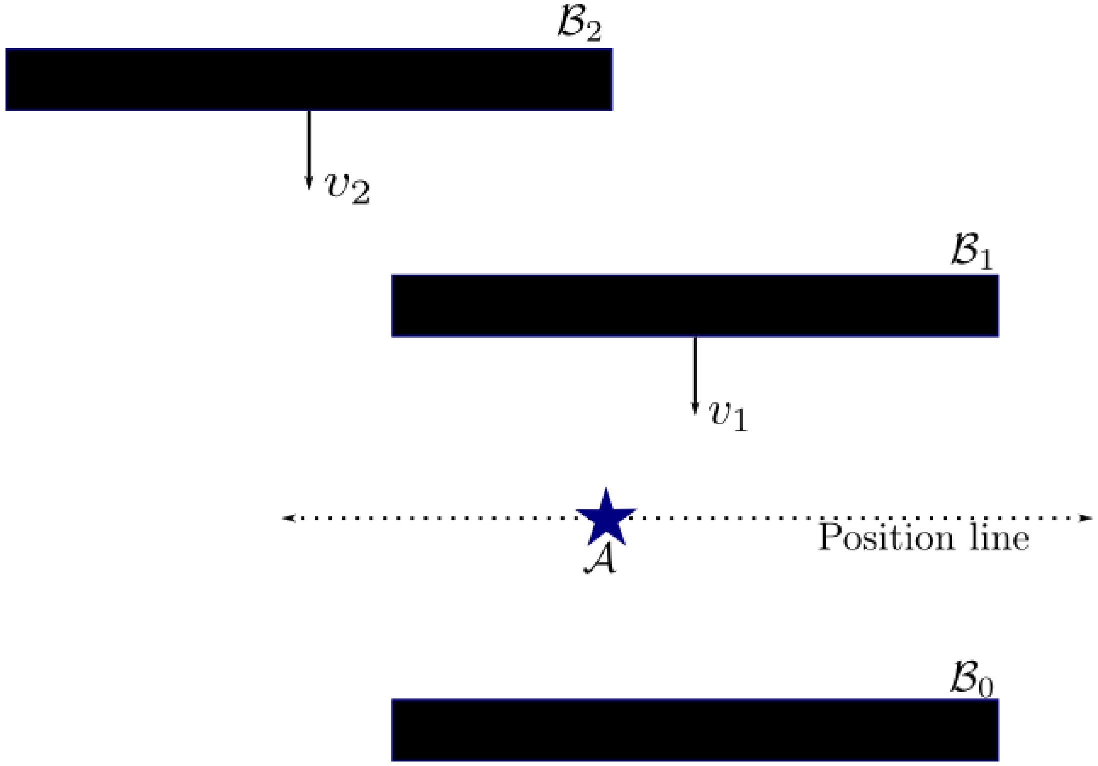
   $\delta_d = t_c | s(s_0, \pi, t_c) \in ICS$, where $\pi$ is the current trajectory

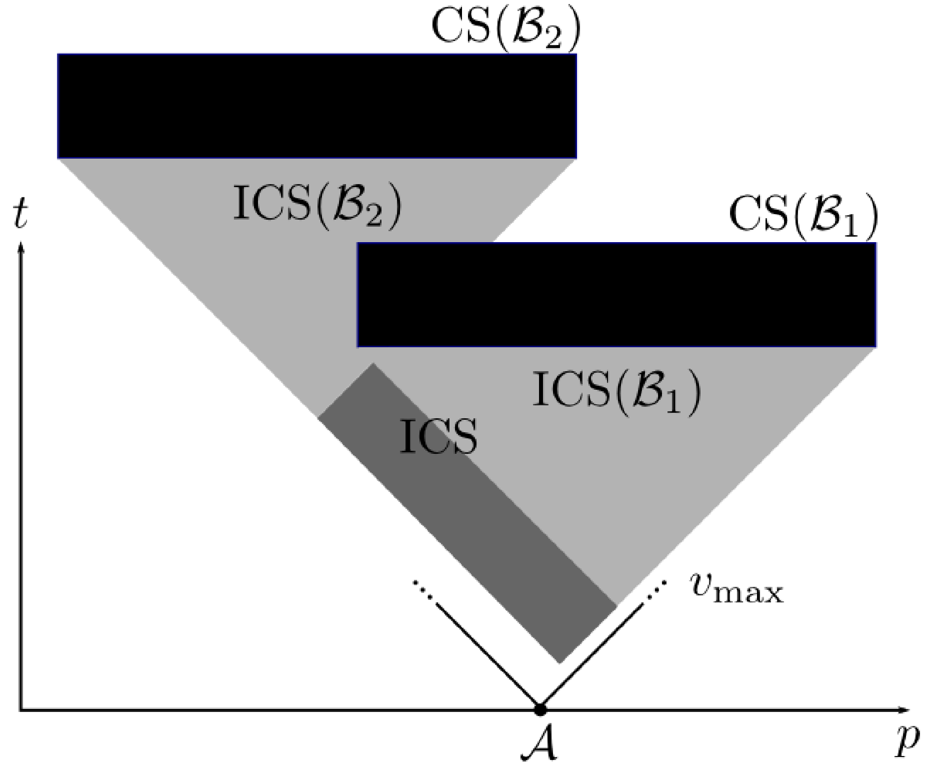
3. Time Horizon

   $\delta_h = t_h | ICS(\mathcal{B}[0, \infty]) \subseteq ICS(\mathcal{B}[0, t_h])$

   Static/freezing/periodic environments $\Rightarrow$ $\delta_d$ not infinite

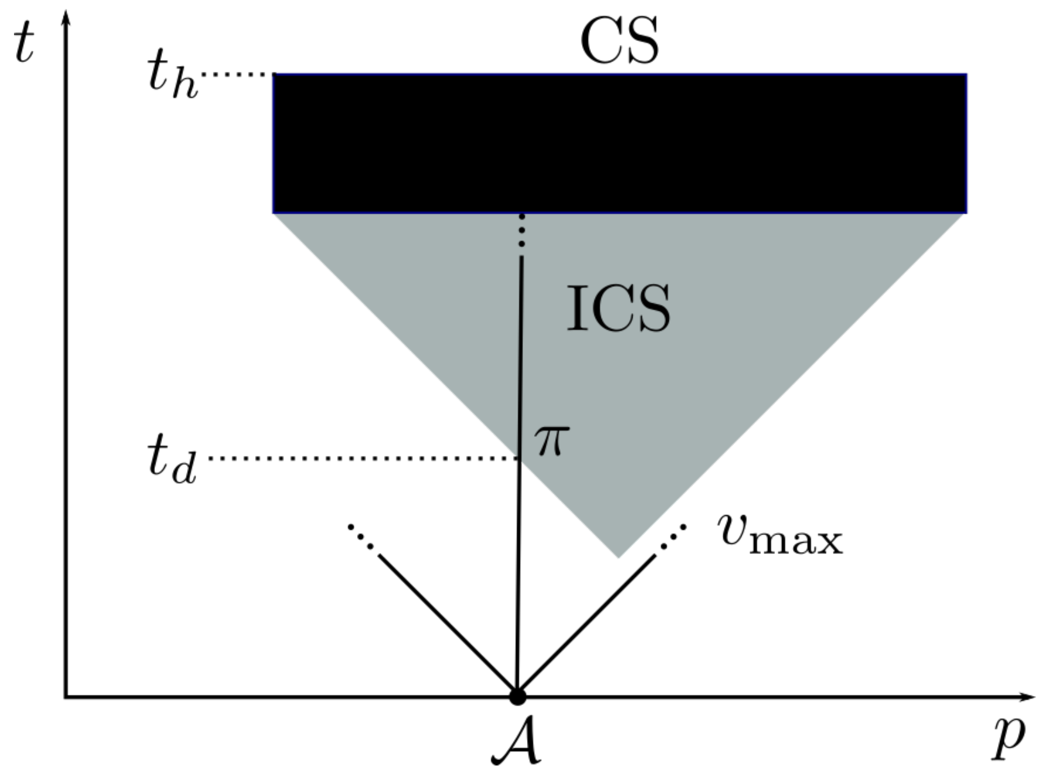
# Obstacles are not Independent




$$\mathrm{ICS}\ (\mathcal{B}_1 \cup \mathcal{B}_2) \supseteq \mathrm{ICS}\ (\mathcal{B}_1) \cup \mathrm{ICS}\ (\mathcal{B}_2)$$

# Decision Time and Time Horizon




$$\begin{cases} \delta_d = t_d \\ \delta_h = t_h \text{ since } ICS(\mathcal{B}[0,\infty]) \subseteq ICS(\mathcal{B}[0,t_h]) \end{cases}$$

# What Have We Learned?

1. Global reasoning about the future evolution of the environment until an appropriate time horizon $\delta_h$, limited decision time $\delta_d$
2. Absolute motion safety = stay away from ICS
3. *ICS = f(*CS*[0,* $\delta_d$*])*
4. *CS = g(B[0,* $\delta_d$*])*
5. $\delta_d$ infinite (except for static/freezing/periodic environments)

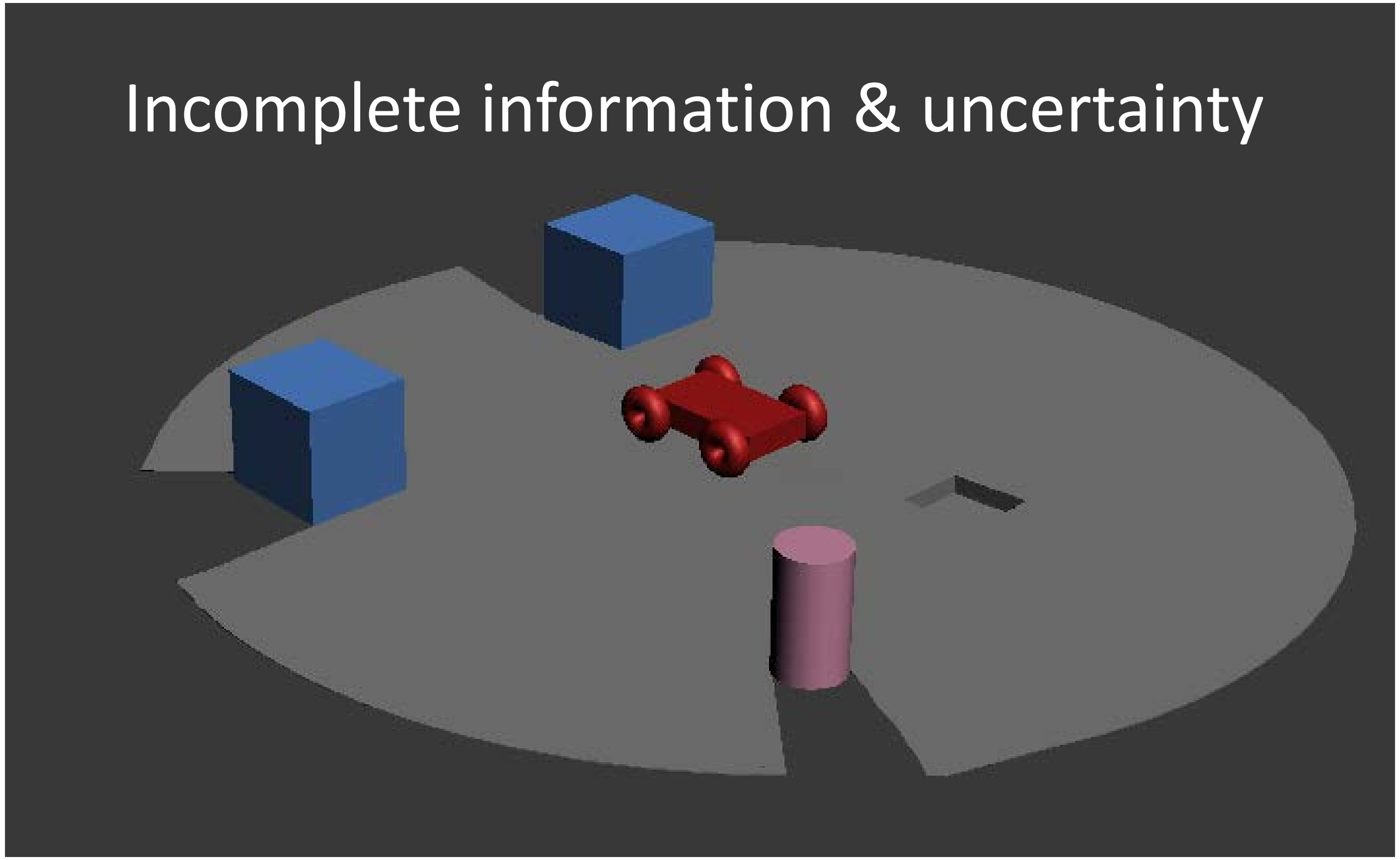
*[Martinez & Fraichard 08]*: robot controller in a static/freezing/periodic environment $\Rightarrow$ guaranteed absolute motion safety

# 3

## Motion Safety in the Real World

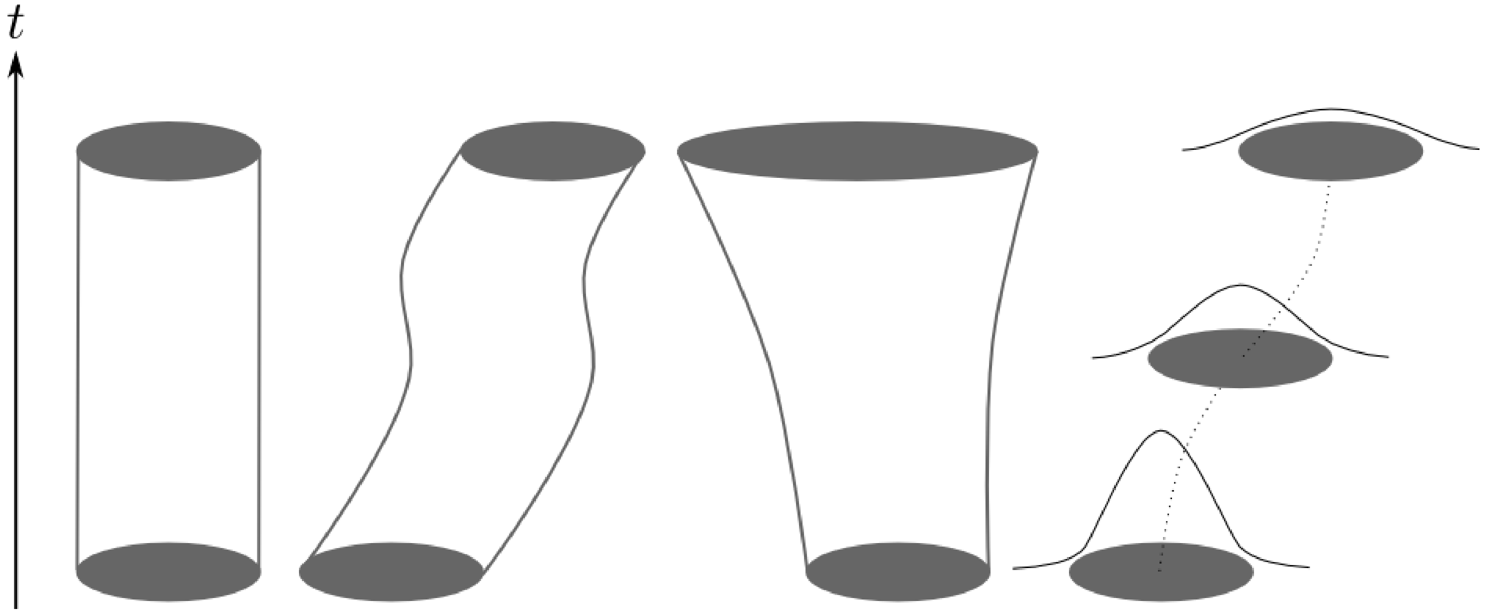
*Houston, we have a problem*

# What about Real World Situations?




$$\mathcal{B}[0, \infty]?$$

# Modeling the Future



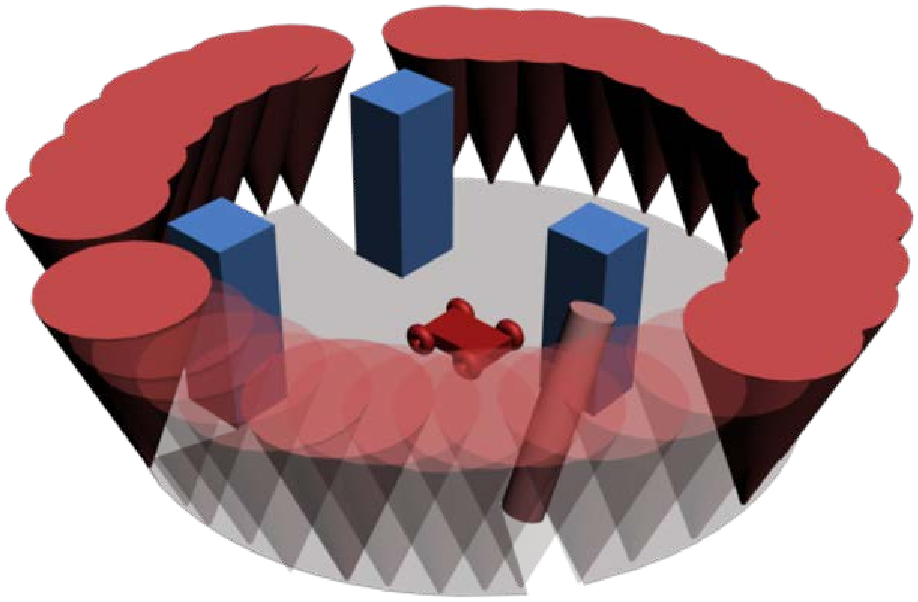

Deterministic Conservative Probabilistic

# Consequences wrt. Motion Safety

- For guaranteed motion safety:
  Conservative model

➢ Every state is an *ICS* $(\delta_h=\infty)$

- What can be done then?
  …Weaker motion safety levels



# 4

## Weaker Motion Safety Levels

*Less is better than nothing*

# Passive Motion Safety

- Should a collision take place, the robot will be at rest
- Braking ICS *[Bouraine & Fraichard, 11]*

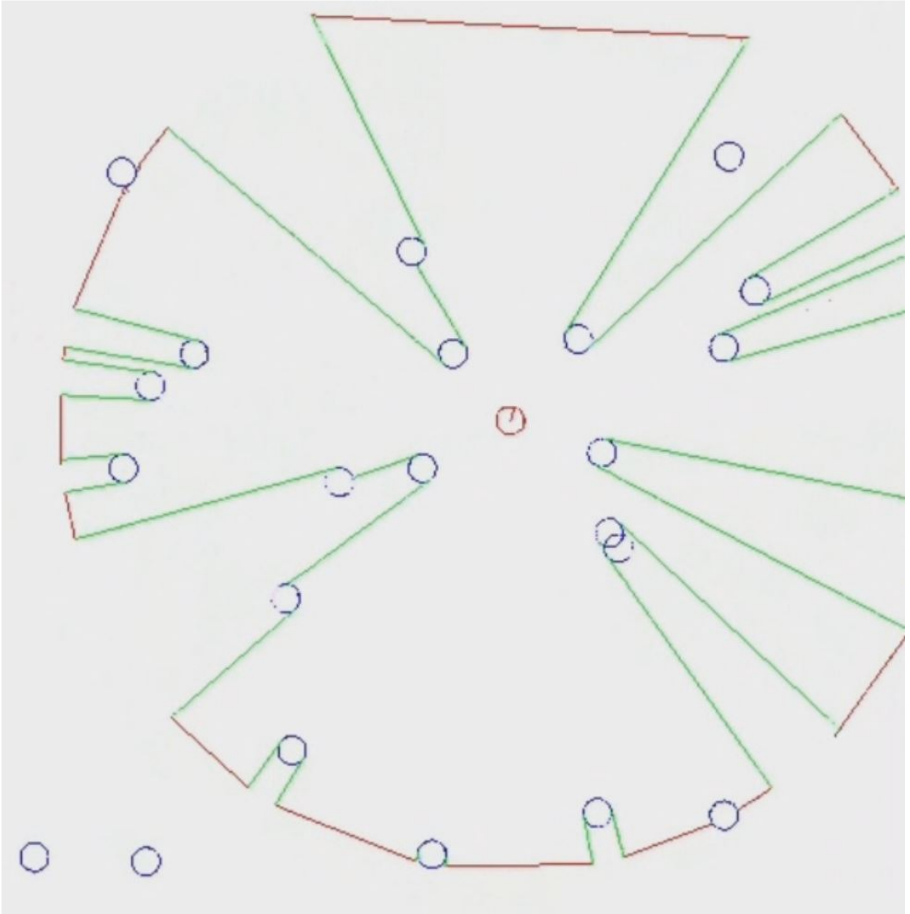
$$\mathcal{A}\text{: state } s \in \mathcal{S}\text{, control } u \in \mathcal{U}\text{, braking trajectory: } \pi_b : [t_0, t_b] \longrightarrow \mathcal{U}$$

$$\text{State } s_0 \text{ is a Braking ICS iff } \forall \pi_b, \exists t \in [0, t_b], s(s_0, \pi, t) \in \text{CS}$$

- Key to passive motion safety: **stay away from Braking ICS**
- Finite time horizon: $max\{t_b\}$
- Everybody enforces it $\Rightarrow$ no collision at all

# Passive Motion Safety can be Guaranteed

- [Provably Safe Navigation for Mobile Robots with Limited Field-of-Views in Dynamic Environments, Bouraine et al., AR, 12]
  - ✓ Dynamic system
  - ✓ Braking ICS



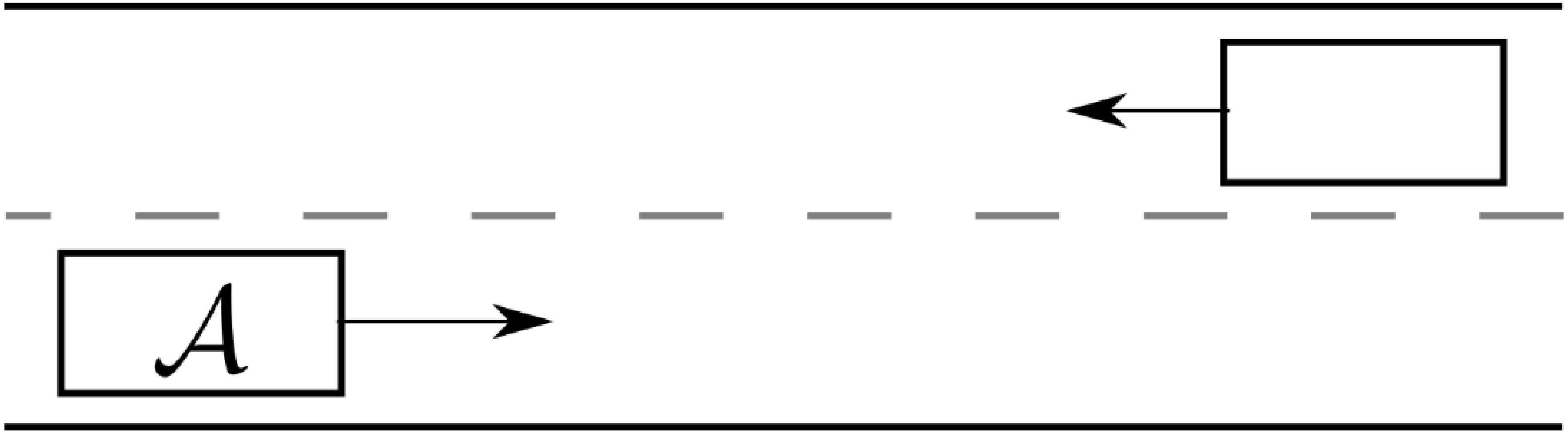
# What about Formal Methods?

- [Formal Verification of Obstacle Avoidance and Navigation of Ground Robots, Mitsch et al., IJRR, 17]
    - ✓ Hybrid system
    - ✓ Differential dynamic logic

**Model 1** Dynamic window with passive safety

$$\begin{aligned}
dw_{\mathrm{ps}} &\equiv (ctrl; dyn)^* && (1)\\
ctrl &\equiv ctrl_o \;||\; ctrl_r && (2)\\
ctrl_o &\equiv v_o := (*,*);\ ?\|v_o\| \le V && (3)\\
ctrl_r &\equiv (a_r := -b) && (4)\\
&\quad \cup (?v_r = 0;\ a_r := 0;\ \omega_r := 0) && (5)\\
&\quad \cup (a_r := *;\ ?{-b} \le a_r \le A; && (6)\\
&\qquad \omega_r := *;\ ?-\Omega \le \omega_r \le \Omega; && (7)\\
&\qquad p_c := (*,*);\ d_r := (*,*); && (8)\\
&\qquad p_o := (*,*);\ ?curve \wedge safe) && (9)\\
curve &\equiv \|p_r - p_c\| > 0 \wedge \omega_r\|p_r - p_c\| = v_r && (10)\\
&\quad \wedge d_r = \frac{(p_r - p_c)^{\perp}}{\|p_r - p_c\|}\\
safe &\equiv \|p_r - p_o\|_{\infty} > \frac{v_r^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon v_r\right) && (11)\\
&\quad + V\left(\varepsilon + \frac{v_r + A\varepsilon}{b}\right) && (12)\\
dyn &\equiv (t := 0;\ p_r^{x\prime} = v_r d_r^x,\ p_r^{y\prime} = v_r d_r^y, && (13)\\
&\qquad d_r^{x\prime} = -\omega_r d_r^y,\ d_r^{y\prime} = \omega_r d_r^x, && (14)\\
&\qquad p_o^{x\prime} = v_o^x,\ p_o^{y\prime} = v_o^y, && (15)\\
&\qquad v_r' = a_r,\ \omega_r' = \frac{a_r}{\|p_r - p_c\|},\ t' = 1 && (16)\\
&\qquad \&\ v_r \ge 0 \wedge t \le \varepsilon) && (17)
\end{aligned}$$

# Passive Motion Safety and Self-Driving Cars



# Time to Conclude

- In the real world, forget guaranteed absolute motion safety
- Guaranteed lesser motion safety possible but…
- Possible improvements: V2V, V2I,roadway engineering

- Self-Driving cars: ~1.4 million miles (Google, up until now), 1 death
- Regular cars: ~3 trillion miles, 30 057 deaths (USA, 2014)

➢ 1 death/100 million miles

Technology still has to prove itself…