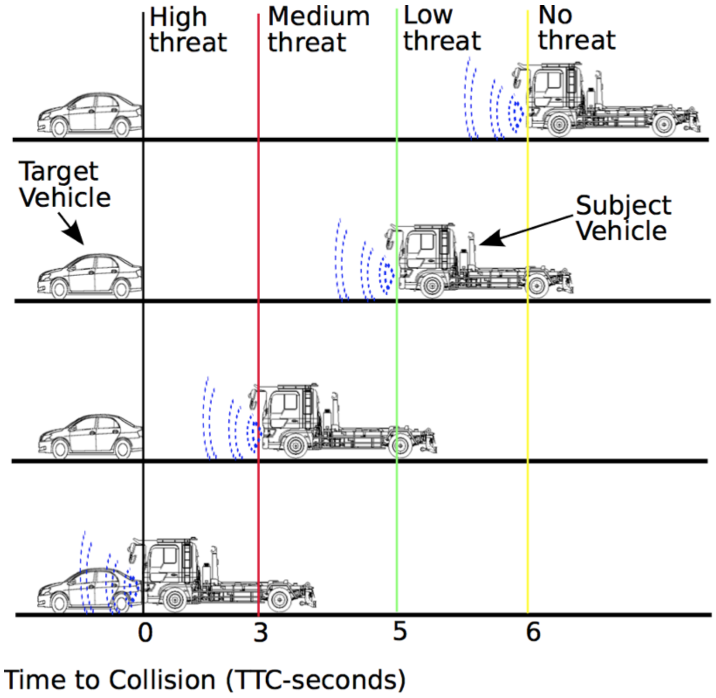
# Automatic Emergency Breaking

## Basic setting

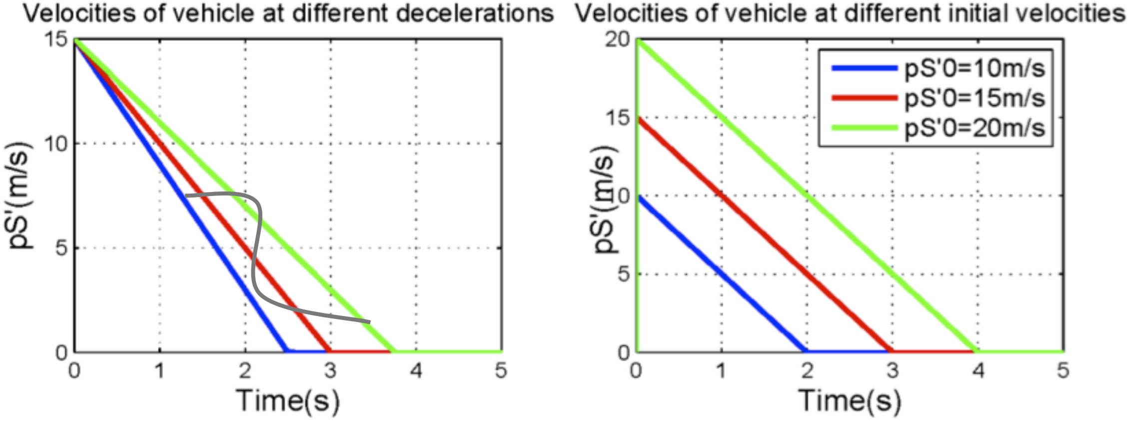
- A rear-endding scenario
- Risks: Sensing & braking failure
- Calculate severity level according to ISO-26262

## Typical variations:

1. Target vehicle stationary, $v_t=0$
2. Target vehicle co-mobile, $0<v_t<v$



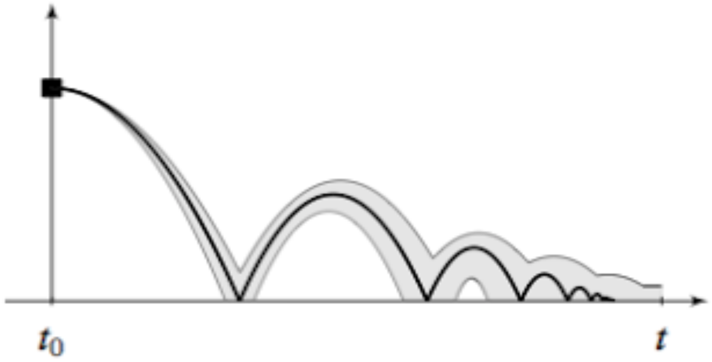
# Traditional Simulation




Key sources of difficulty:

- Numerical approximation
- Parameter uncertainty (exponential & infinite)

# Basic Idea: Rigorous Enclosures

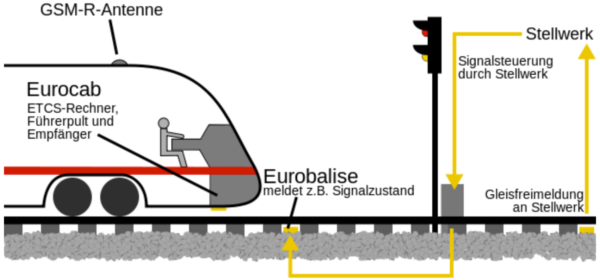


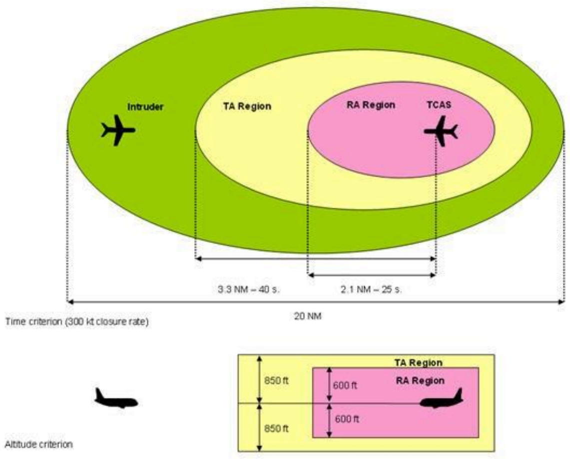

- Bound system behaviour
- The bound is guaranteed (rigorous)
- Explicitly account for numerical errors
- Provide a natural model for uncertainty

# Rest of this talk

- Rigorous simulation
- Acumen
- Design time verification
- Results
- Conclusions

# State of the Art in Verification

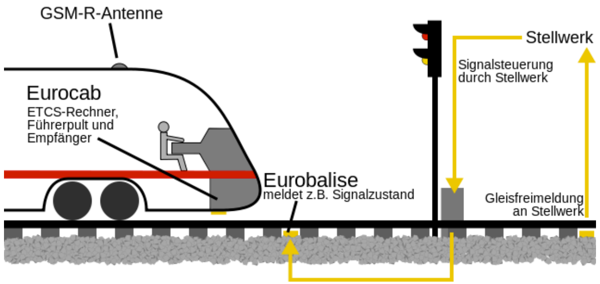


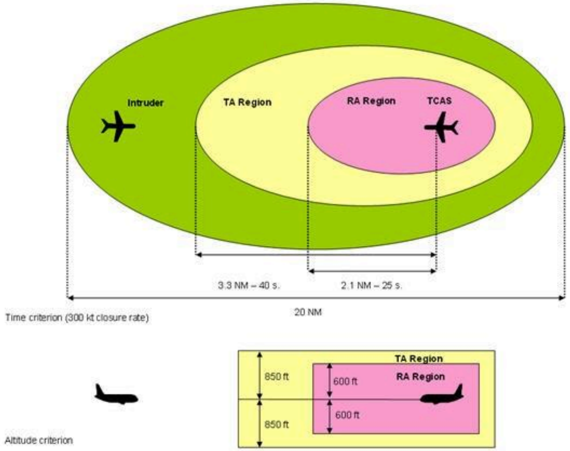




Example of ACAS Protection Volume between 5000 and 10000 feet

The Good: We have Proofs!

# State of the Art in Verification

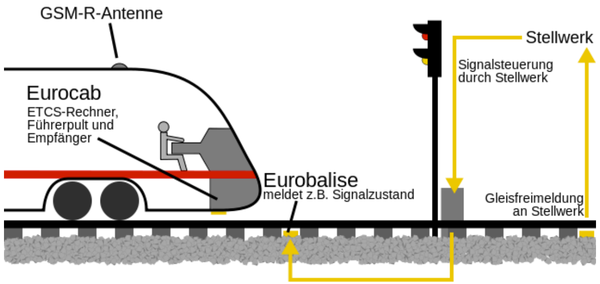


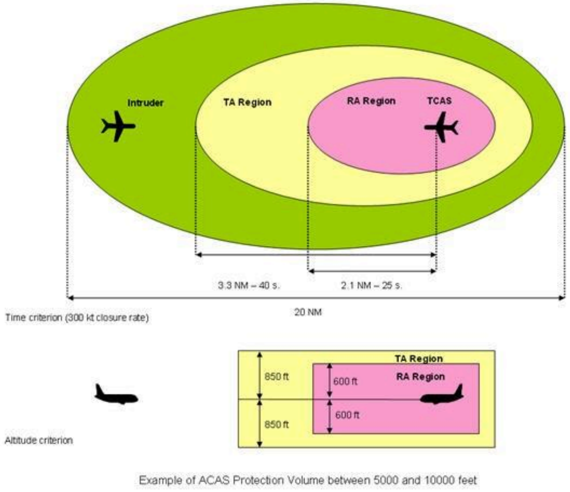




Example of ACAS Protection Volume between 5000 and 10000 feet

The Bad: Can only handle very small systems

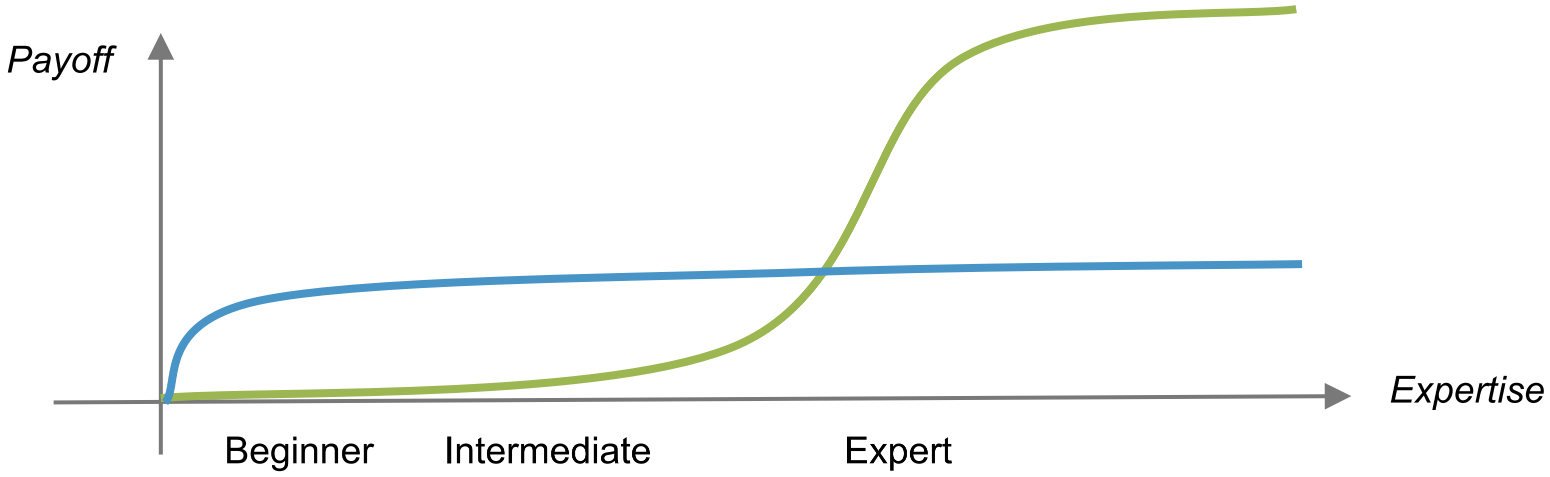
# State of the Art in Verification



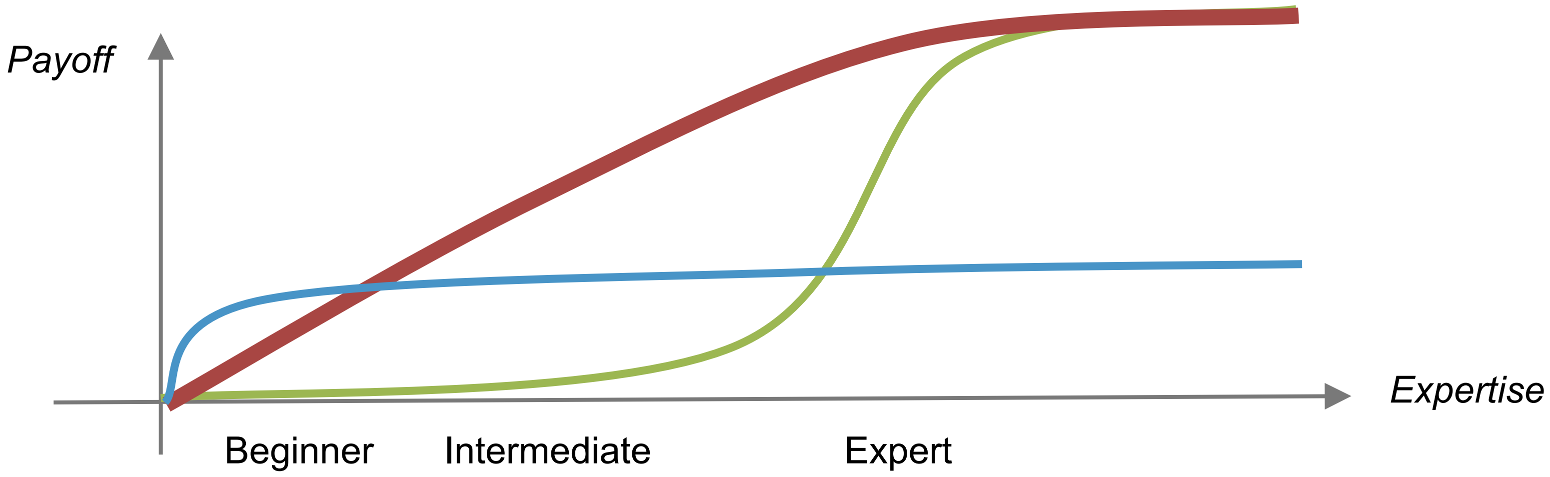

The Ugly:  Very effort intensive, need Gurus

# Usability of Verification Tools



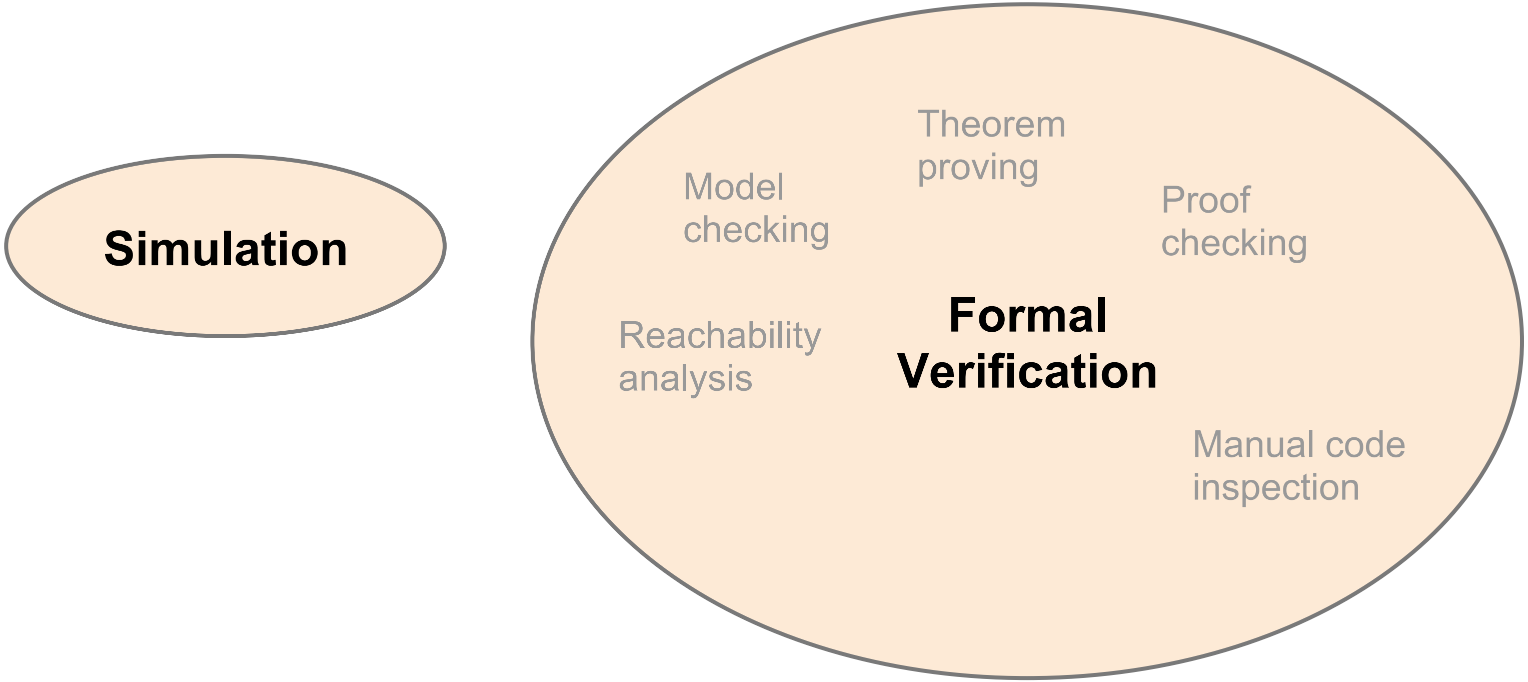

Generally, verification tools require a very high level of sophistication on the side of the user *before* any positive payoff is possible.

# Usability of Verification Tools

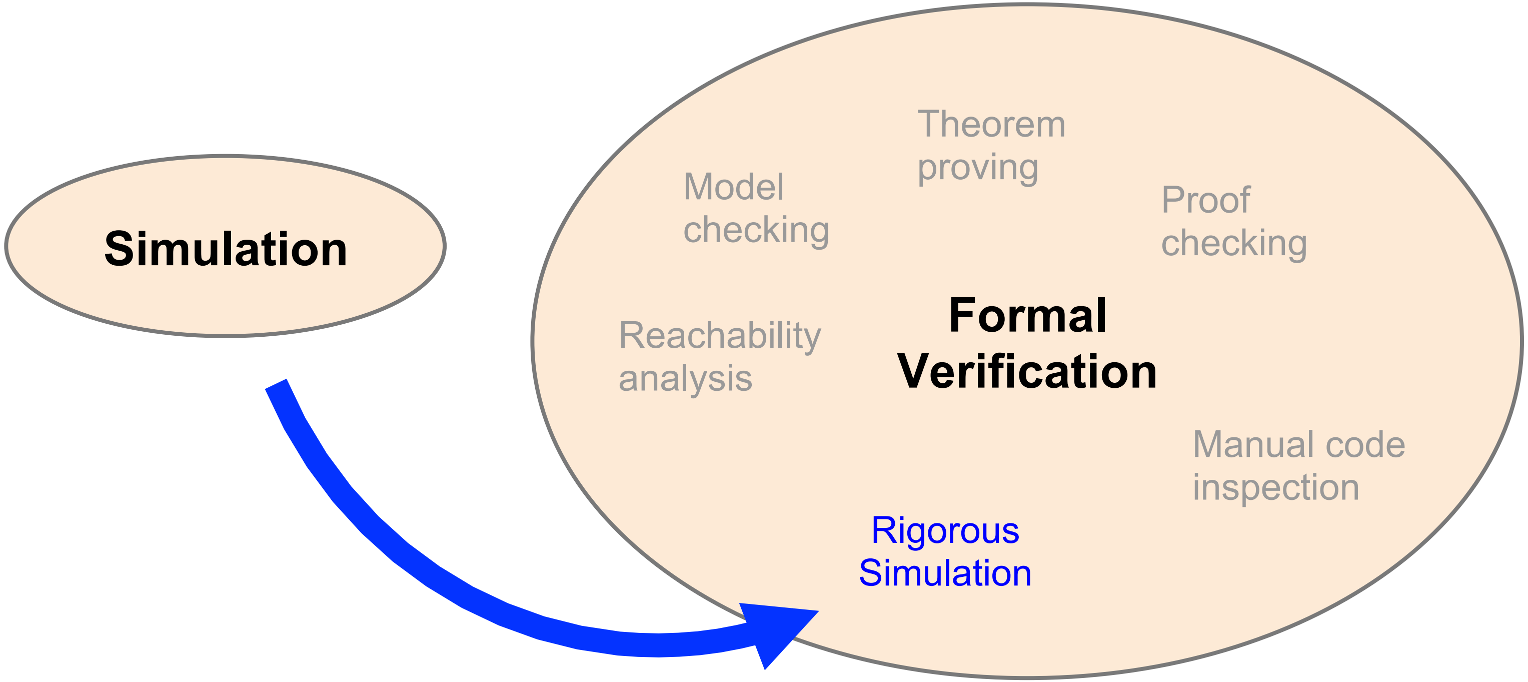



We propose **rigorous simulation** as a way to make verification accessible: start with a readily accessible approach (simulation).

# Simulation and Verification



# Simulation and Verification



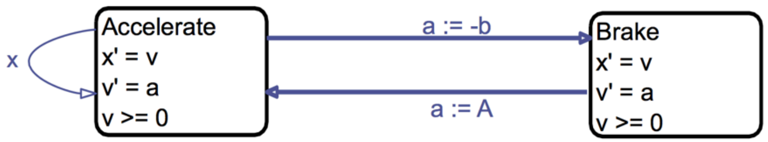
# Acumen

- Small domain specific language
- Offer solution to simple differential equations using
  - Floating point
  - Interval arithmetic using enclosures
- User can visualize solution (plots, 3D visualization)
- Open source (BSD license)
- Link: http://www.acumen-language.org/

# Acumen Enclosures

Hybrid system specifies:

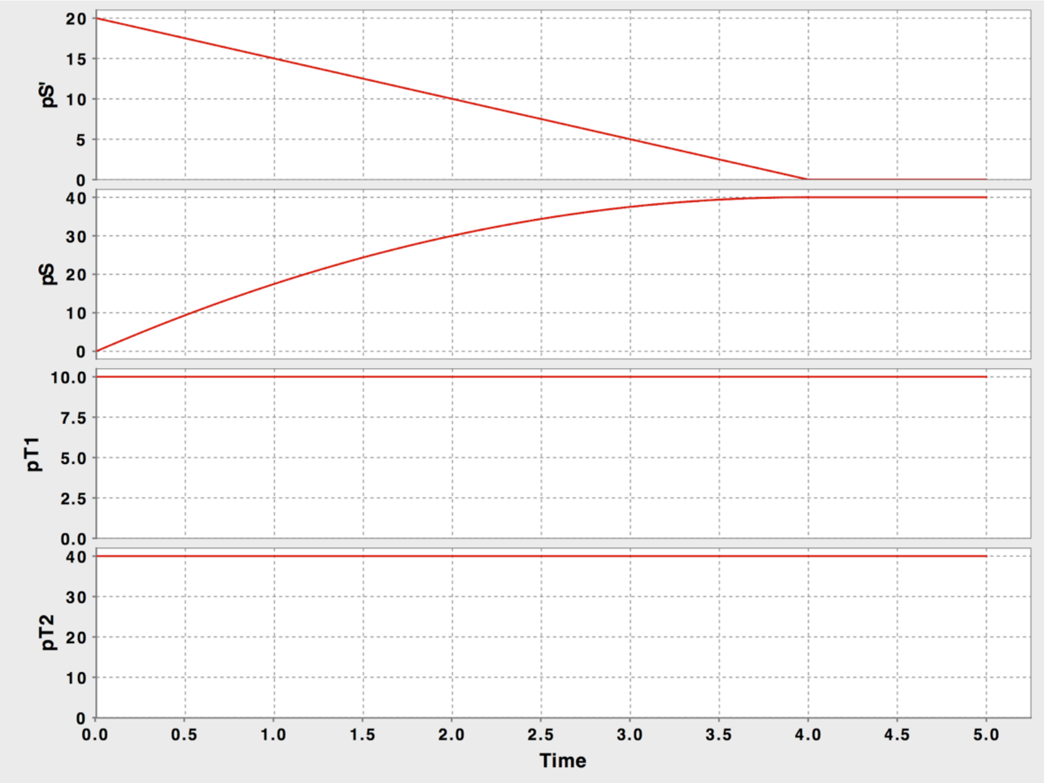
- Initial state
- Differential equations
- Continuous and discrete
- Switching conditions



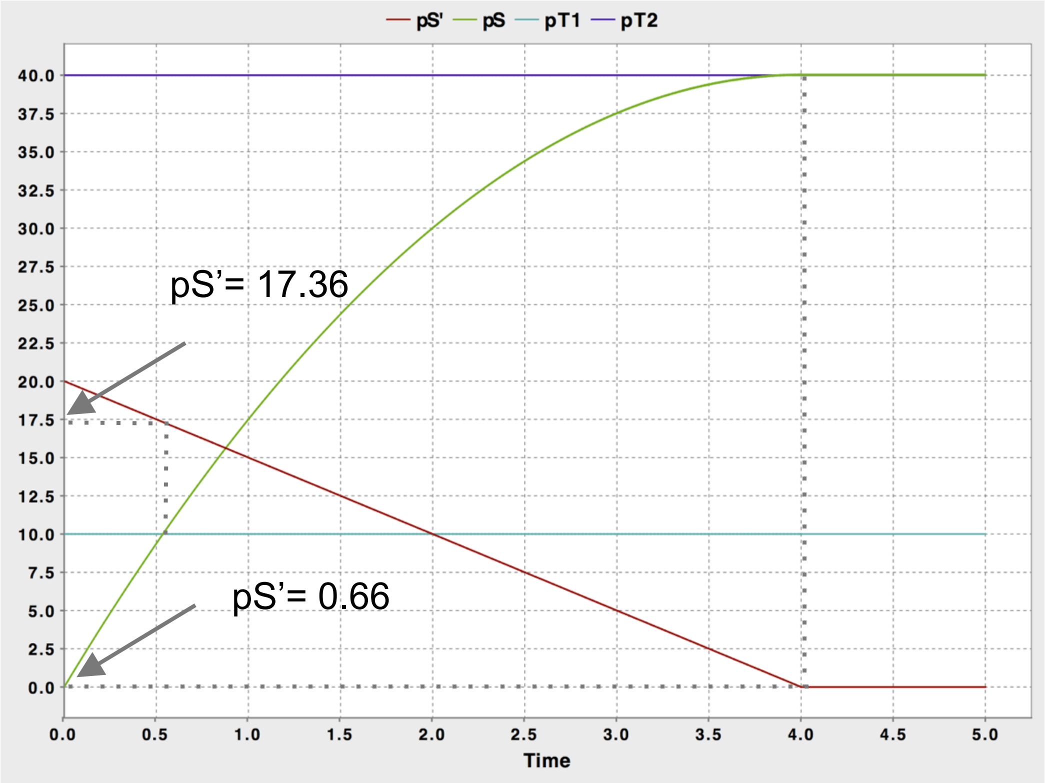

Enclosures with soundness guarantee:

- Solution to differential equations
- Switching conditions correct valuation

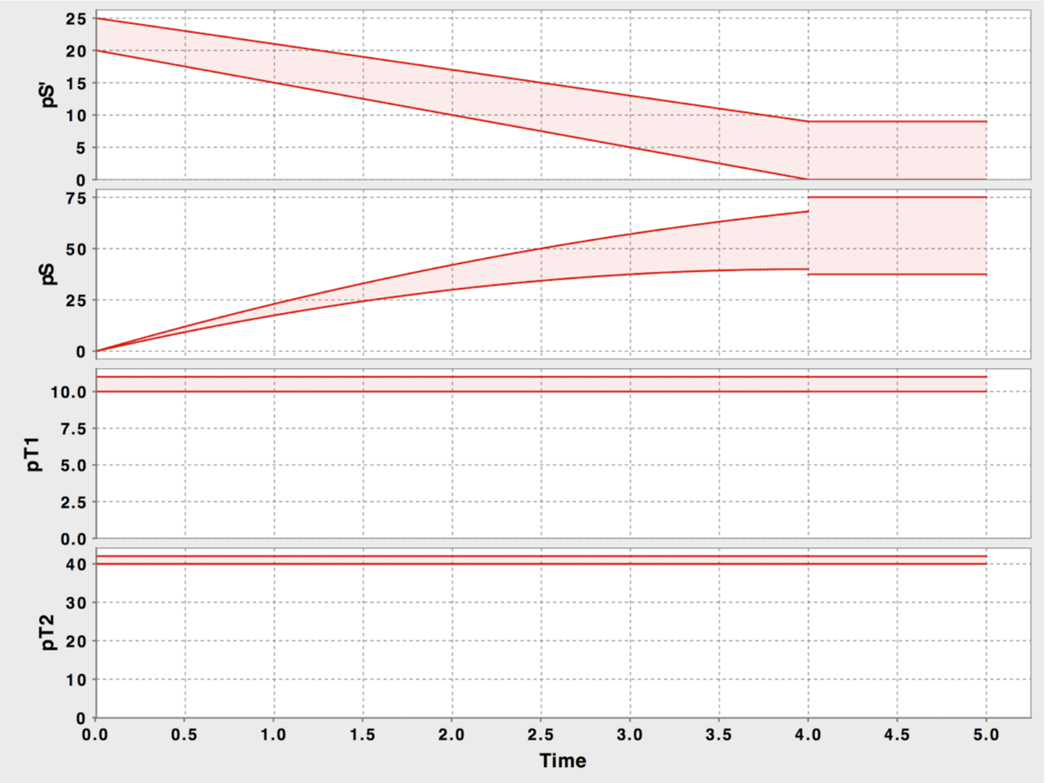
# Traditional Simulation



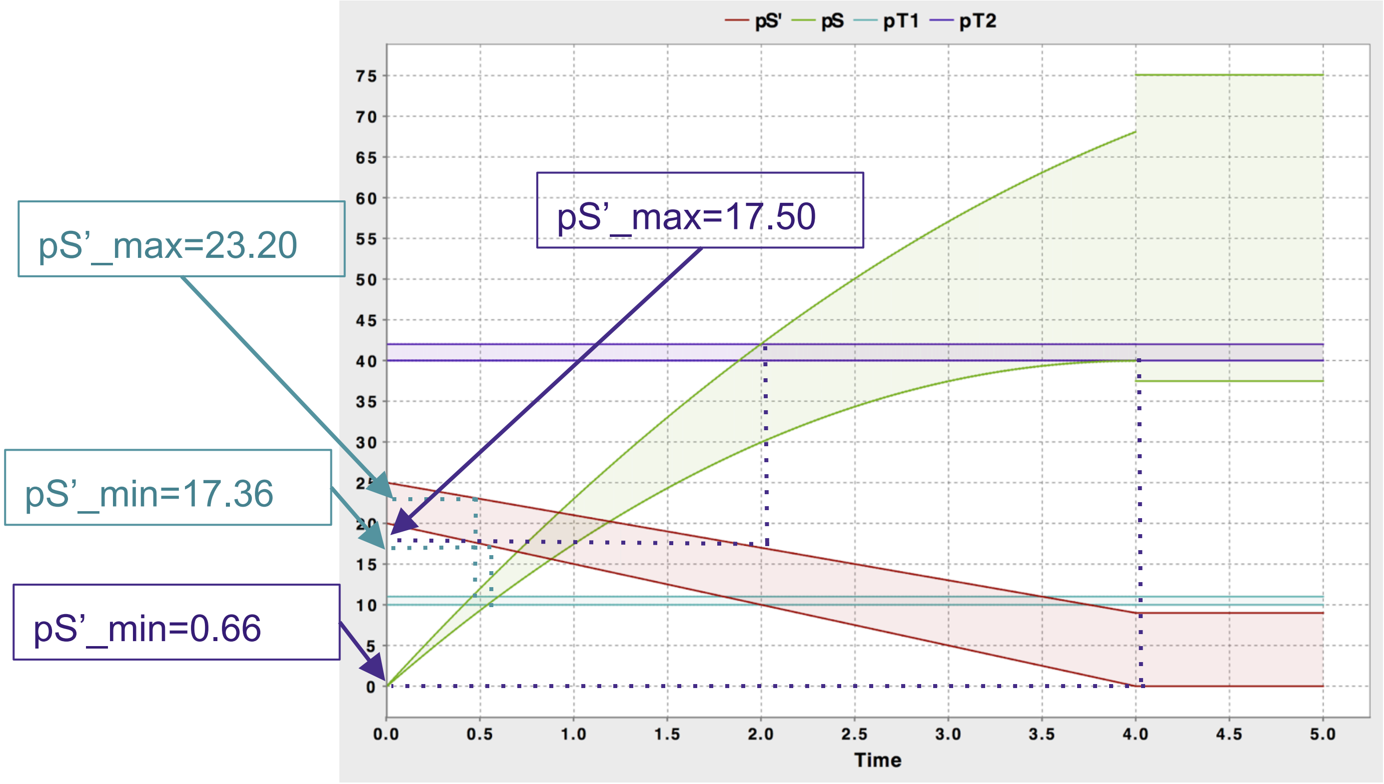
# Traditional Simulation



# Rigorous Simulation

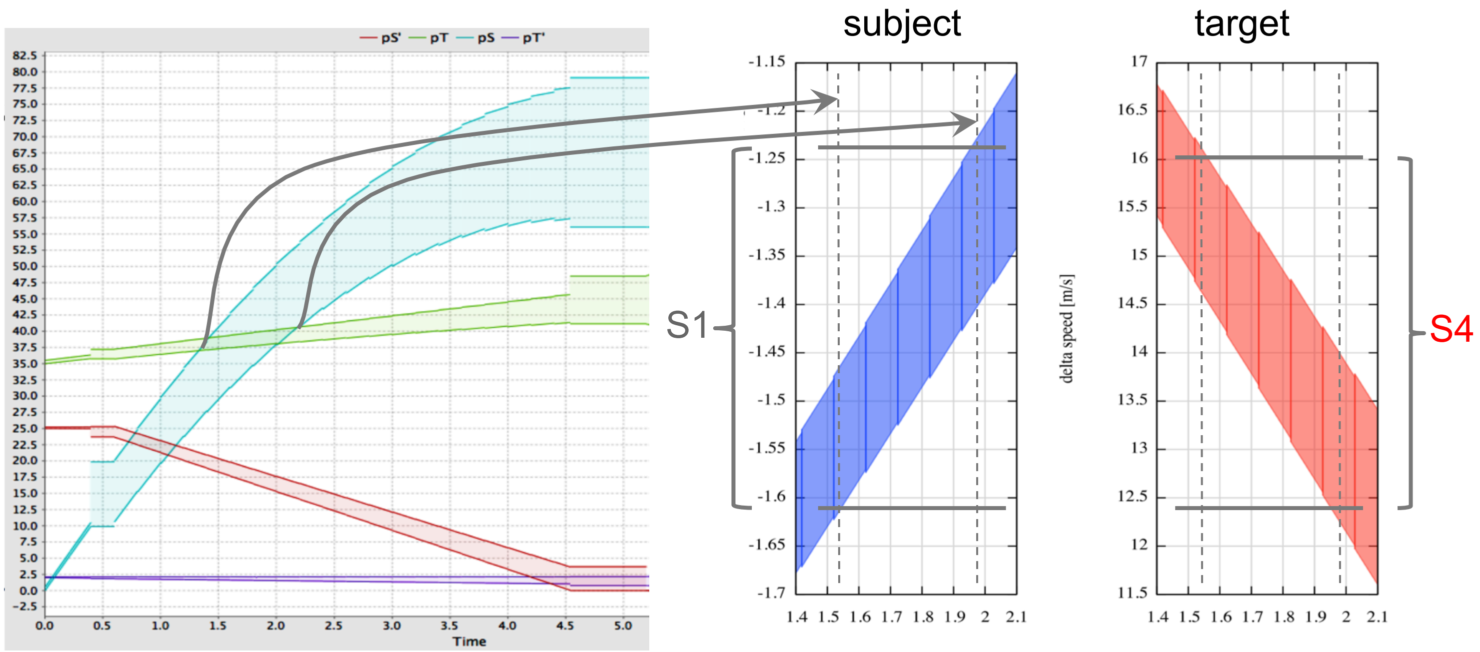


# Rigorous Simulation - Case 1



# Rigorous Simulation - Case 2

- 8 interval variables
- Inelastic collision



# Severity level - Scenario 1, $v_t$=0

$$\Delta \dot{p}_S = \frac{M_T(\dot{p}_T - \dot{p}_S)}{M_T + M_S}, \Delta \dot{p}_T = \frac{M_S(\dot{p}_S - \dot{p}_T)}{M_T + M_S}$$

| Scenario | Target Vehicle: mass 2,000 kg | | Subject Vehicle: mass 10,000 kg | | System Verification |
|---|---|---|---|---|---|
| Case | $\Delta p'_T$ (Delta V) km/h | ISO-26262 Severity Level | $\Delta p'_s$ (Delta V) km/h | ISO-26262 Severity Level | $S_0$, $S_1$ or $S_2$ => Compliance => Pass<br>$S_3$ or $S_4$ => Compliance => Fail |
| Initial target vehicle position $p_T$ = 10±0.5m | {52.0,69.5} | $\{S_4,S_4\}$ | {10.2,13.9} | $\{S_2,S_2\}$ | AEB system fails under ISO-26262 |
| Initial target vehicle position $p_T$ = 41±0.5m | {2.0,50.8} | $\{S_0,S_4\}$ | {0.4,10.2} | $\{S_0,S_2\}$ | AEB system fails under ISO-26262 |

# Severity level - Scenario 2, $v_t < v_s$

$$\Delta \dot{p_S} = \frac{M_T(\dot{p_T} - \dot{p_S})}{M_T + M_S},\ \Delta \dot{p_T} = \frac{M_S(\dot{p_S} - \dot{p_T})}{M_T + M_S}$$

| Scenario | Target Vehicle: mass 2,000 kg | | Subject Vehicle: mass 10,000 kg | | System Verification |
|---|---|---|---|---|---|
| Case | $\Delta p'_T$ (Delta V) km/h | ISO-26262 Severity Level | $\Delta p'_s$ (Delta V) km/h | ISO-26262 Severity Level | $S_0$, $S_1$ or $S_2$ => Compliance => Pass<br>$S_3$ or $S_4$ => Compliance => Fail |
| Initial target vehicle position $p_T$ = 35±0.5m | {41.8,55.4}, {48.2,59.8} | $\{S_4,S_4\}$, $\{S_4,S_4\}$ | {4.6,5.6}, {4.8,6.0} | $\{S_0,S_1\}$, $\{S_0,S_1\}$ | AEB system fails under ISO-26262 |

# Conclusions

- Rigorous simulation is a powerful tool
- Being rigorous makes it **a verification tool**
- … and means implementation correctness is critical
- Being based on simulation makes it **easy to use**
- … also makes it **relatively fast**
- Naturally accommodates **parametric uncertainty**
- … which makes simulations **much more informative**
- Using rigorous simulation during easy-stage design has a distinctive flavor that **promotes robust design**