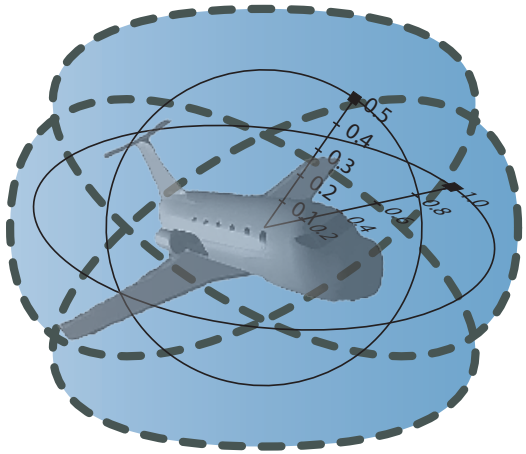
15-819/18-879: Logical Analysis of Hybrid Systems

01: Hybrid Systems Applications

André Platzer

aplatzer@cs.cmu.edu
Carnegie Mellon University, Pittsburgh, PA



Outline

1. Hybrid Systems Applications
   - Air Traffic Control
   - Hybrid Systems / Cyber-Physical Systems
   - Train Control
   - Car Control
   - UAV
   - Chemical/Physical Process Control
   - Biomedical Applications
   - Advanced Chip Design

How can we build computerized controllers for physical systems that are guaranteed to meet their design goals?

About 15-819/18-879

- Hybrid systems
- Logical analysis
- Symbolic / numerical techniques
- Automatic theorem proving
- Model checking
- Verification
- Balance theory, practice & applications
- 30% Homework, 15% Midterm, 55% Project
- Project: Theory and/or implementation and/or application
- Whitepaper (4p), proposal (10p), report

Course Outline

1. Safety-critical complex physical systems
2. Dynamical systems: discrete, continuous, hybrid
3. Controllability, safety & stability
4. First-order logic and first-order real arithmetic
5. Symbolic reachability analysis
6. Hybrid programs and hybrid automata
7. Dynamic logic & dynamical systems, differential dynamic logic
8. Differential variance and invariance
9. Differential-algebraic equations and differential algebra
10. Differential transformations and differential reductions
11. Railway control applications
12. Air traffic control applications
13. Distributed car control applications

Questionnaire

- Differential equations

Questionnaire

- Differential equations (Peano, Picard-Lindelöff, Cauchy-Lipschitz)

Questionnaire

- Differential equations (Peano, Picard-Lindelöff, Cauchy-Lipschitz)
- First-order logic

Questionnaire

- Differential equations (Peano, Picard-Lindelöff, Cauchy-Lipschitz)
- First-order logic
- Hybrid systems

Questionnaire

- Differential equations (Peano, Picard-Lindelöff, Cauchy-Lipschitz)
- First-order logic
- Hybrid systems
- Deduction & formal proofs

Questionnaire

- Differential equations (Peano, Picard-Lindelöff, Cauchy-Lipschitz)
- First-order logic
- Hybrid systems
- Deduction & formal proofs
- Model checking

Questionnaire

- Differential equations (Peano, Picard-Lindelöff, Cauchy-Lipschitz)
- First-order logic
- Hybrid systems
- Deduction & formal proofs
- Model checking
- Quantifier elimination

Questionnaire

- Differential equations (Peano, Picard-Lindelöff, Cauchy-Lipschitz)
- First-order logic
- Hybrid systems
- Deduction & formal proofs
- Model checking
- Quantifier elimination
- Algebraic geometry

Questionnaire

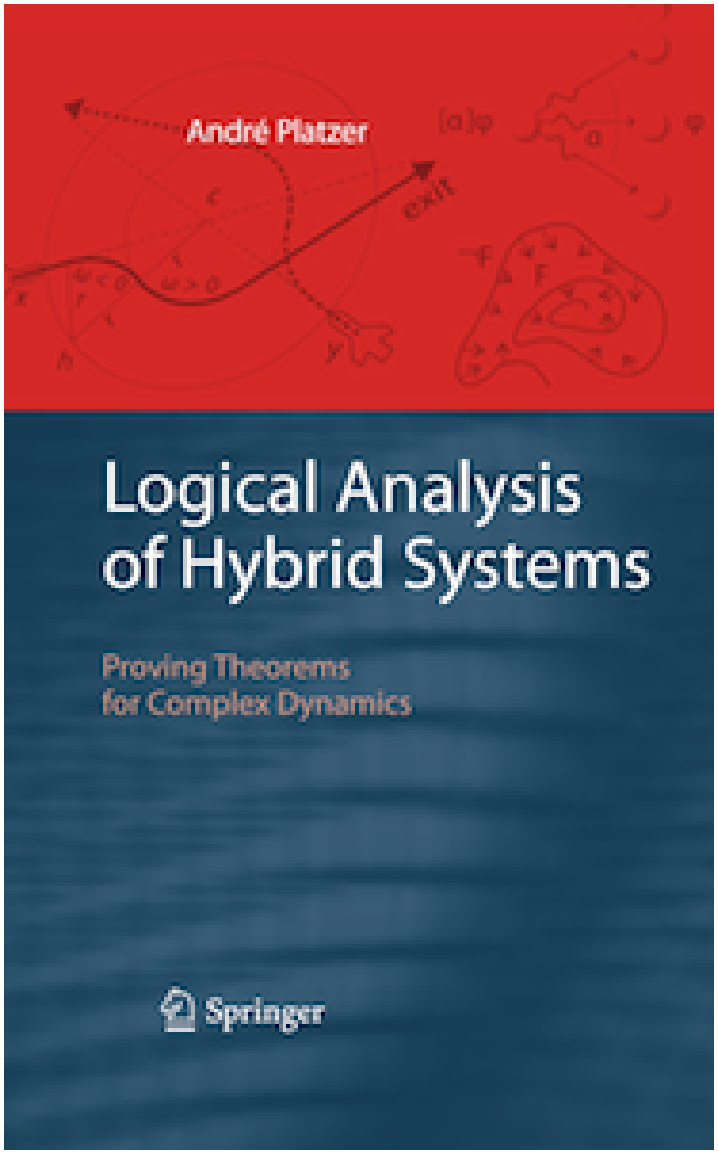
- Differential equations (Peano, Picard-Lindelöff, Cauchy-Lipschitz)
- First-order logic
- Hybrid systems
- Deduction & formal proofs
- Model checking
- Quantifier elimination
- Algebraic geometry
- Differential algebra

Questionnaire

- Differential equations (Peano, Picard-Lindelöff, Cauchy-Lipschitz)
- First-order logic
- Hybrid systems
- Deduction & formal proofs
- Model checking
- Quantifier elimination
- Algebraic geometry
- Differential algebra
- Computer algebra


Logical Analysis of Hybrid Systems
Logic
Proof Calculus
Theorem Proving
Model Checking
Algebra
Computer Algebra
Algebraic Geometry
Differential Algebra
Algorithms
Fixedpoint Loops
Proof Strategies
Decision Procedures
Analysis
Differential Equations
Dynamical Systems
Differen-tiation

Textbook

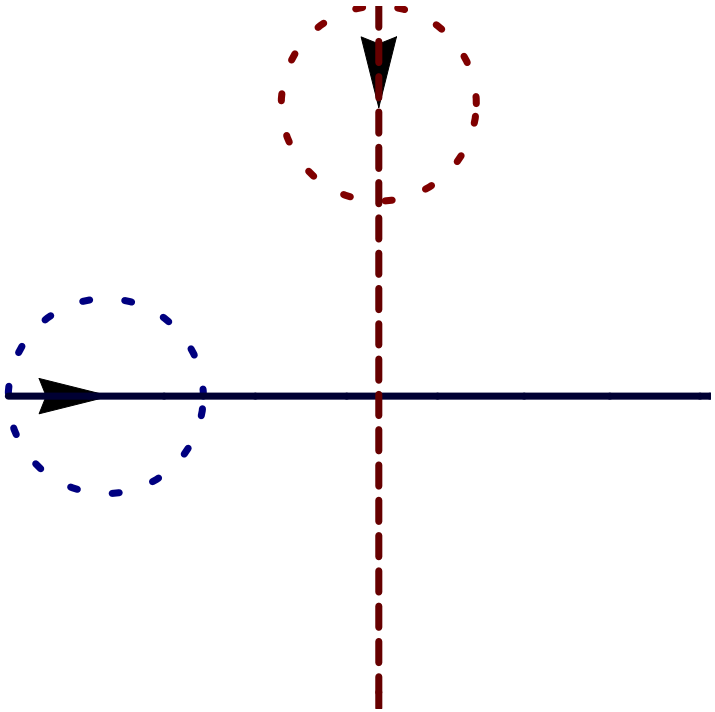


André Platzer.
Logical Analysis of Hybrid Systems.
Springer, 426p., 2010.
ISBN 978-3-642-14508-7.
http://symbolaris.com/lahs/

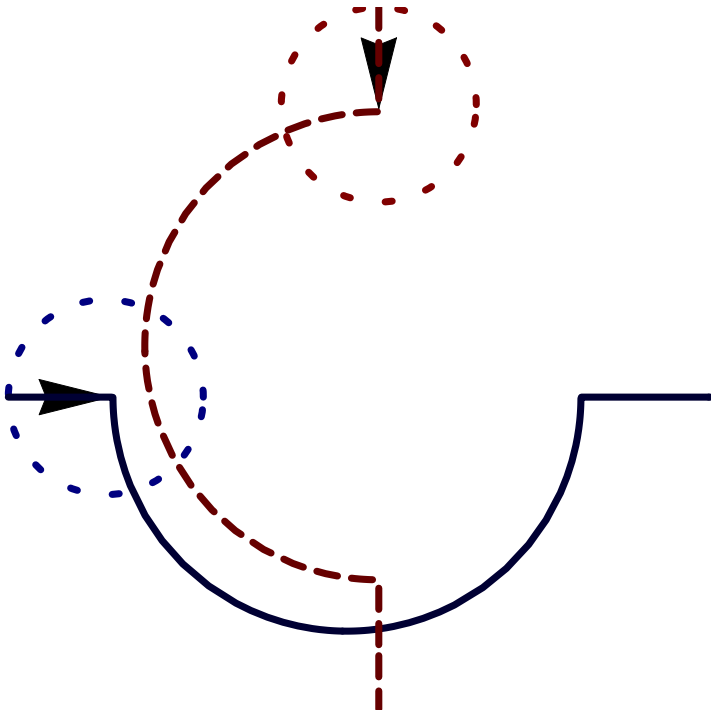
Outline

1. Hybrid Systems Applications
   - Air Traffic Control
   - Hybrid Systems / Cyber-Physical Systems
   - Train Control
   - Car Control
   - UAV
   - Chemical/Physical Process Control
   - Biomedical Applications
   - Advanced Chip Design

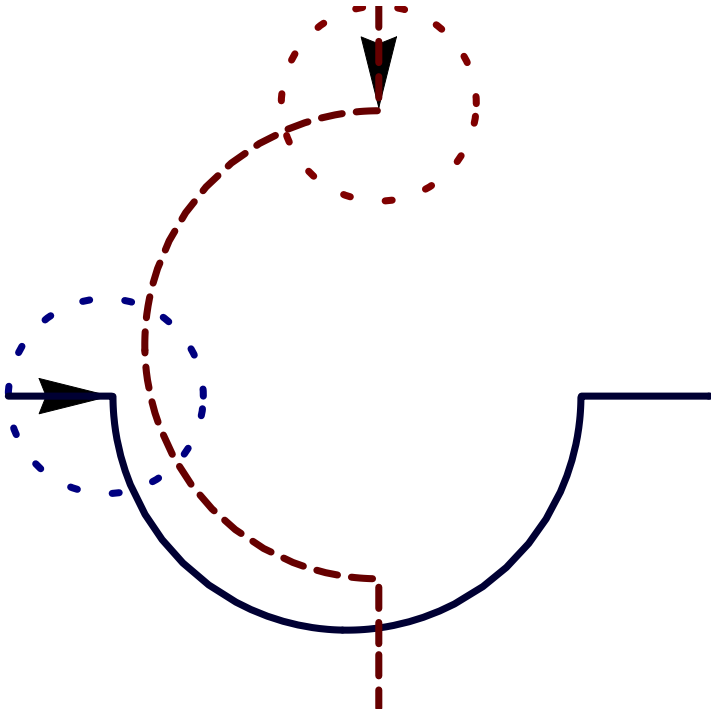
Air Traffic Control



Air Traffic Control



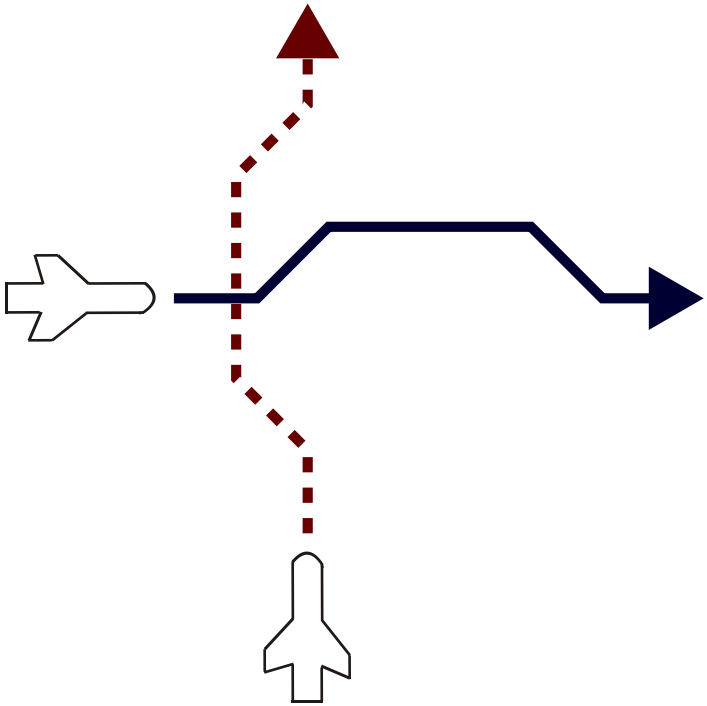
Air Traffic Control

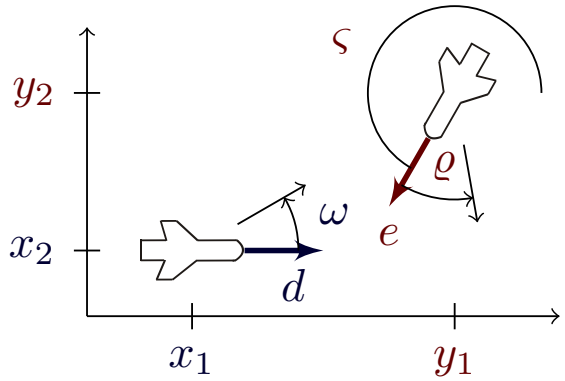


Hybrid Systems

interacting discrete and continuous dynamics

Air Traffic Control



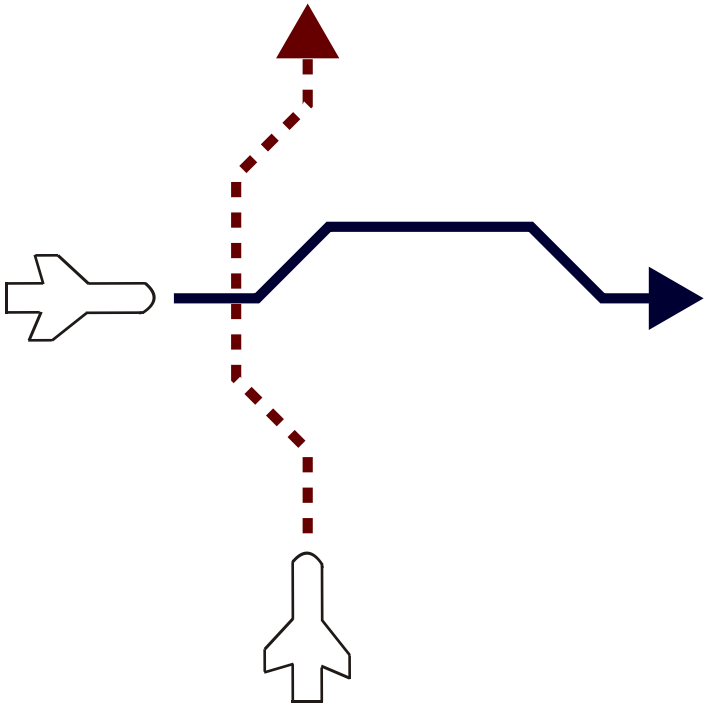


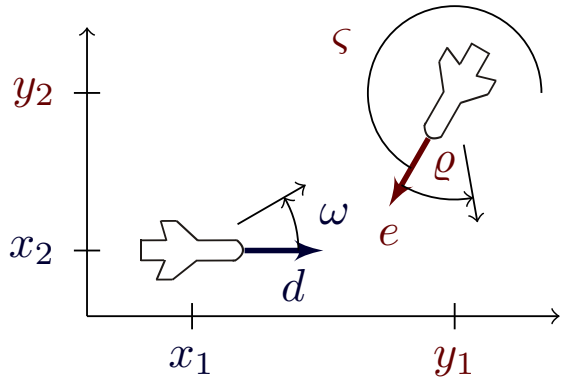
$$\begin{bmatrix} x_1' = v\cos\vartheta & y_1' = u\cos\varsigma \\ x_2' = v\sin\vartheta & y_2' = u\sin\varsigma \end{bmatrix}$$

Hybrid Systems

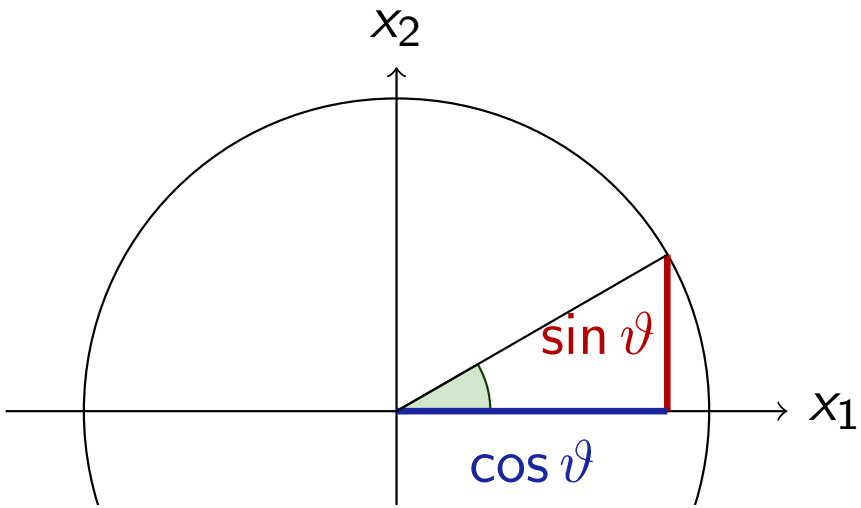
interacting discrete and continuous dynamics

Air Traffic Control

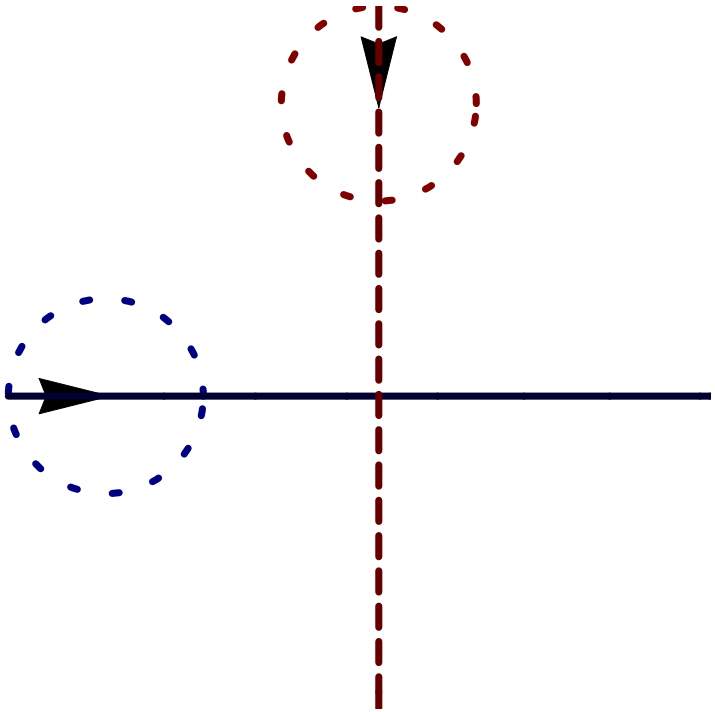




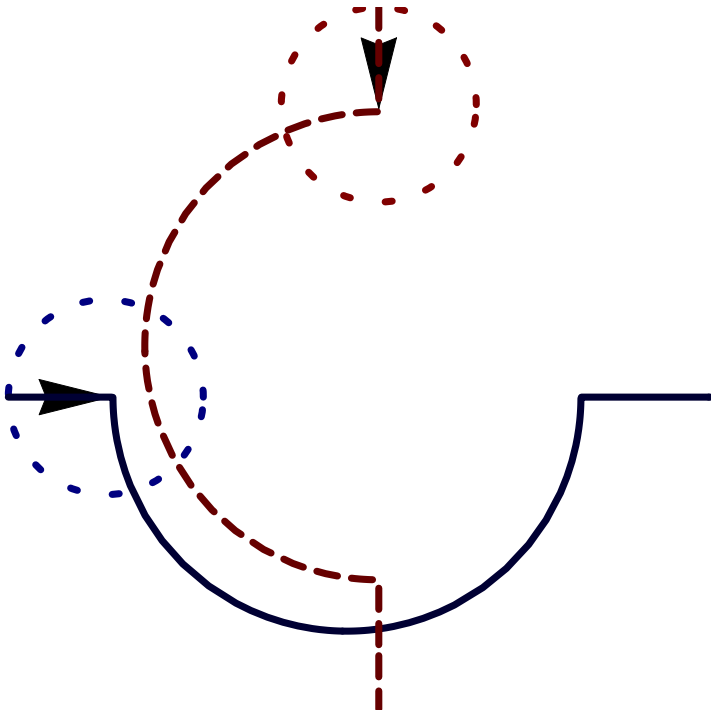
$$\begin{bmatrix} x_1' = v\cos\vartheta & y_1' = u\cos\varsigma \\ x_2' = v\sin\vartheta & y_2' = u\sin\varsigma \end{bmatrix}$$



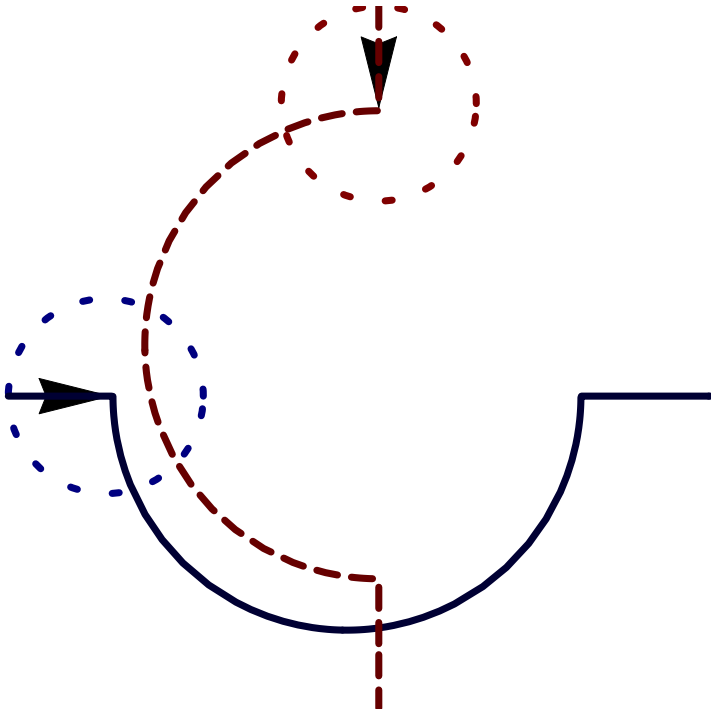
Air Traffic Control



Air Traffic Control



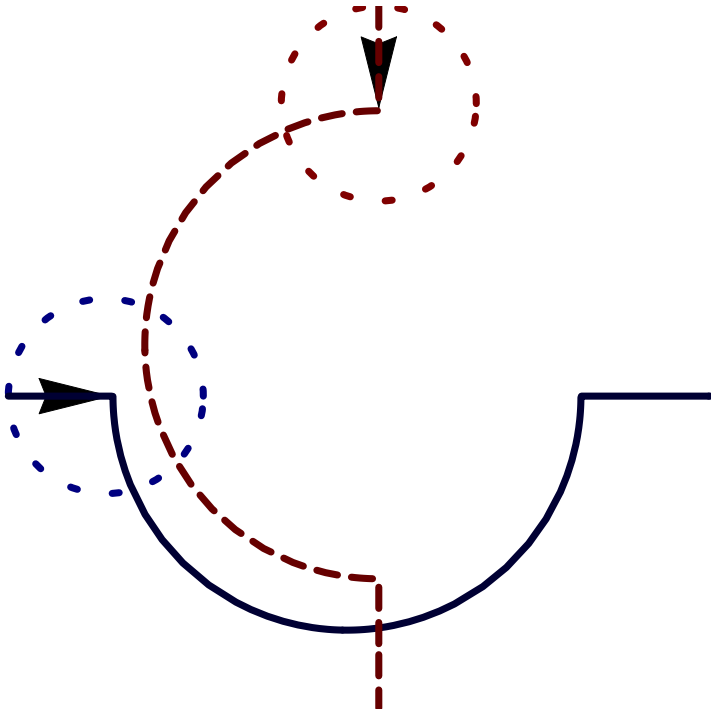
Air Traffic Control

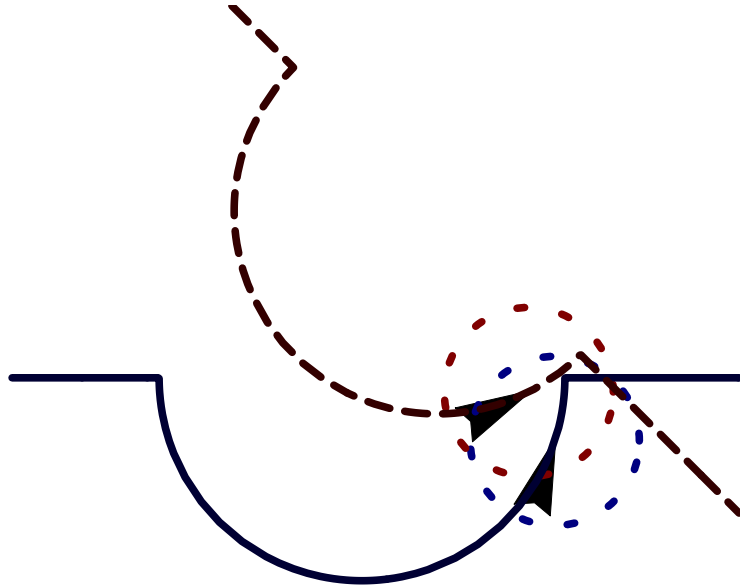


Verification?

looks correct

Air Traffic Control

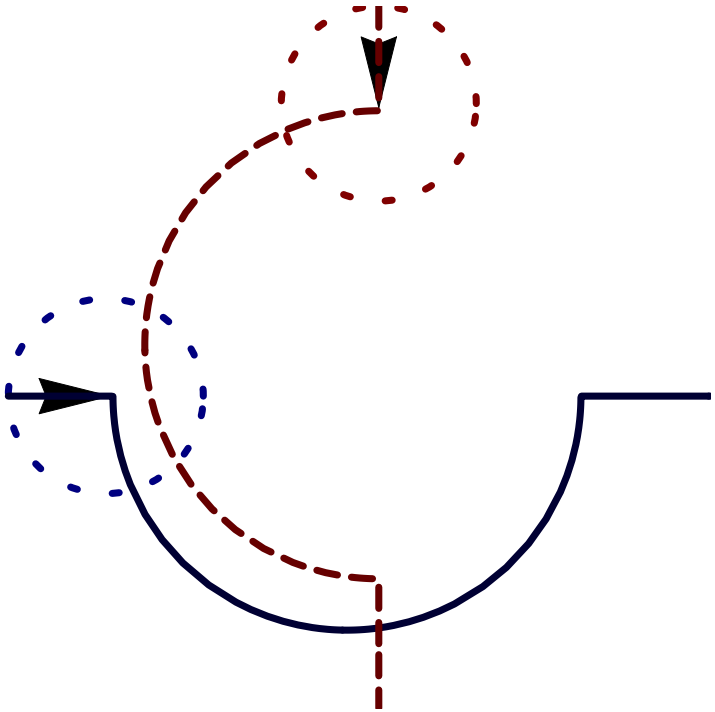


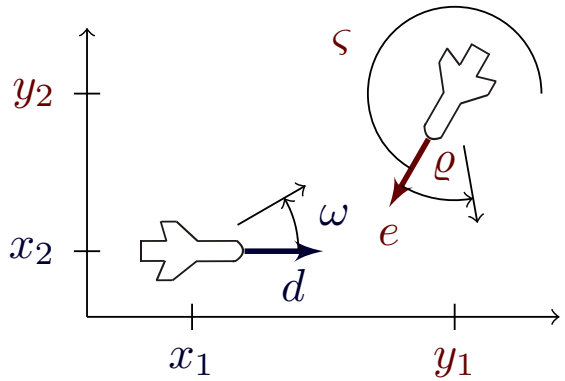


Verification?

looks correct NO!

Air Traffic Control



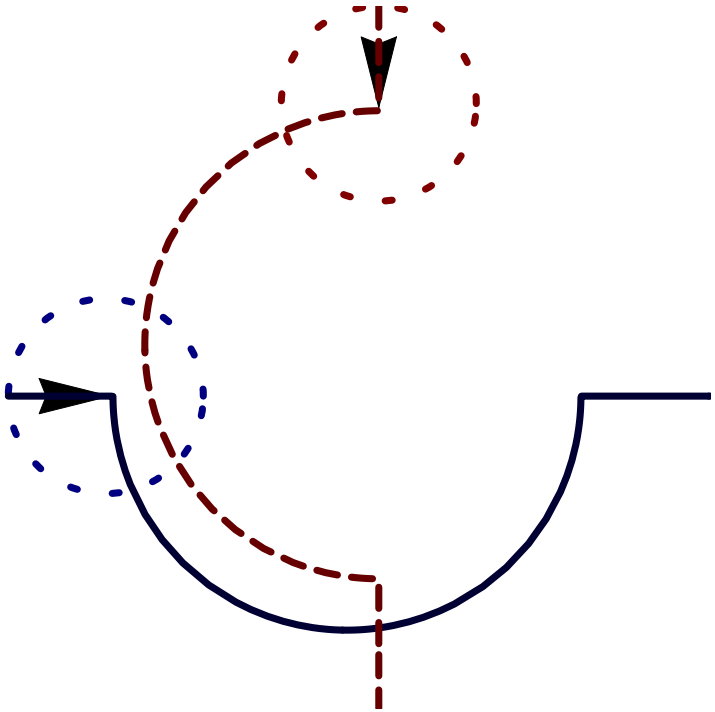


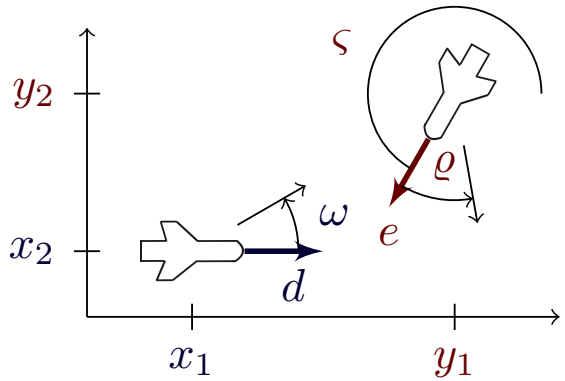
$$\begin{bmatrix} x_1' = -v + u\cos\vartheta + \omega x_2 \\ x_2' = u\sin\vartheta - \omega x_1 \\ \vartheta' = \varpi - \omega \end{bmatrix}$$

Verification?

looks correct NO!

Air Traffic Control



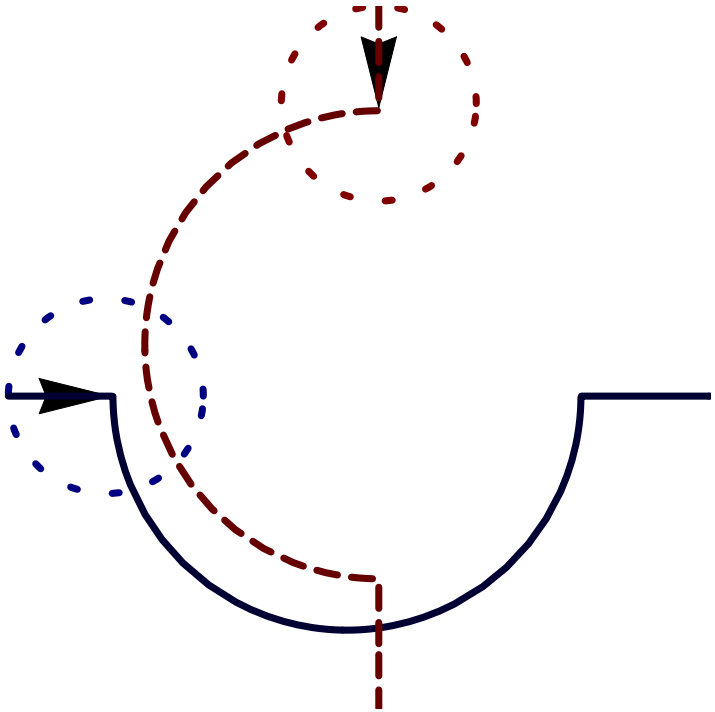


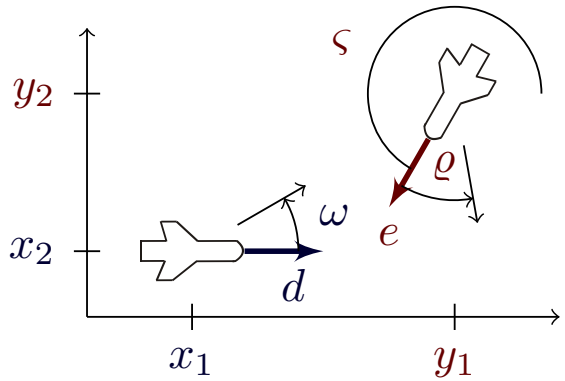
$$\begin{bmatrix} x_1' = -v + u\cos\vartheta + \omega x_2 \\ x_2' = u\sin\vartheta - \omega x_1 \\ \vartheta' = \varpi - \omega \end{bmatrix}$$

Example ("Solving" differential equations)

$$x_1(t) = \frac{1}{\omega\varpi}\big(x_1\omega\varpi\cos t\omega - u\omega\cos t\omega\sin\vartheta + u\omega\cos t\omega\cos t\varpi\sin\vartheta - v\varpi\sin t\omega$$
$$+ x_2\omega\varpi\sin t\omega - u\omega\cos\vartheta\cos t\varpi\sin t\omega - u\omega\sqrt{1-\sin\vartheta^2}\sin t\omega$$
$$+ u\omega\cos\vartheta\cos t\omega\sin t\varpi + u\omega\sin\vartheta\sin t\omega\sin t\varpi\big)\ldots$$

Air Traffic Control





$$\begin{bmatrix} x_1' = -v + u\cos\vartheta + \omega x_2 \\ x_2' = u\sin\vartheta - \omega x_1 \\ \vartheta' = \varpi - \omega \end{bmatrix}$$

Example ("Solving" differential equations)

$\forall t \geq 0$ $\quad \frac{1}{\omega\varpi}\big(x_1\omega\varpi\cos t\omega - u\omega\cos t\omega\sin\vartheta + u\omega\cos t\omega\cos t\varpi\sin\vartheta - v\varpi\sin t\omega$

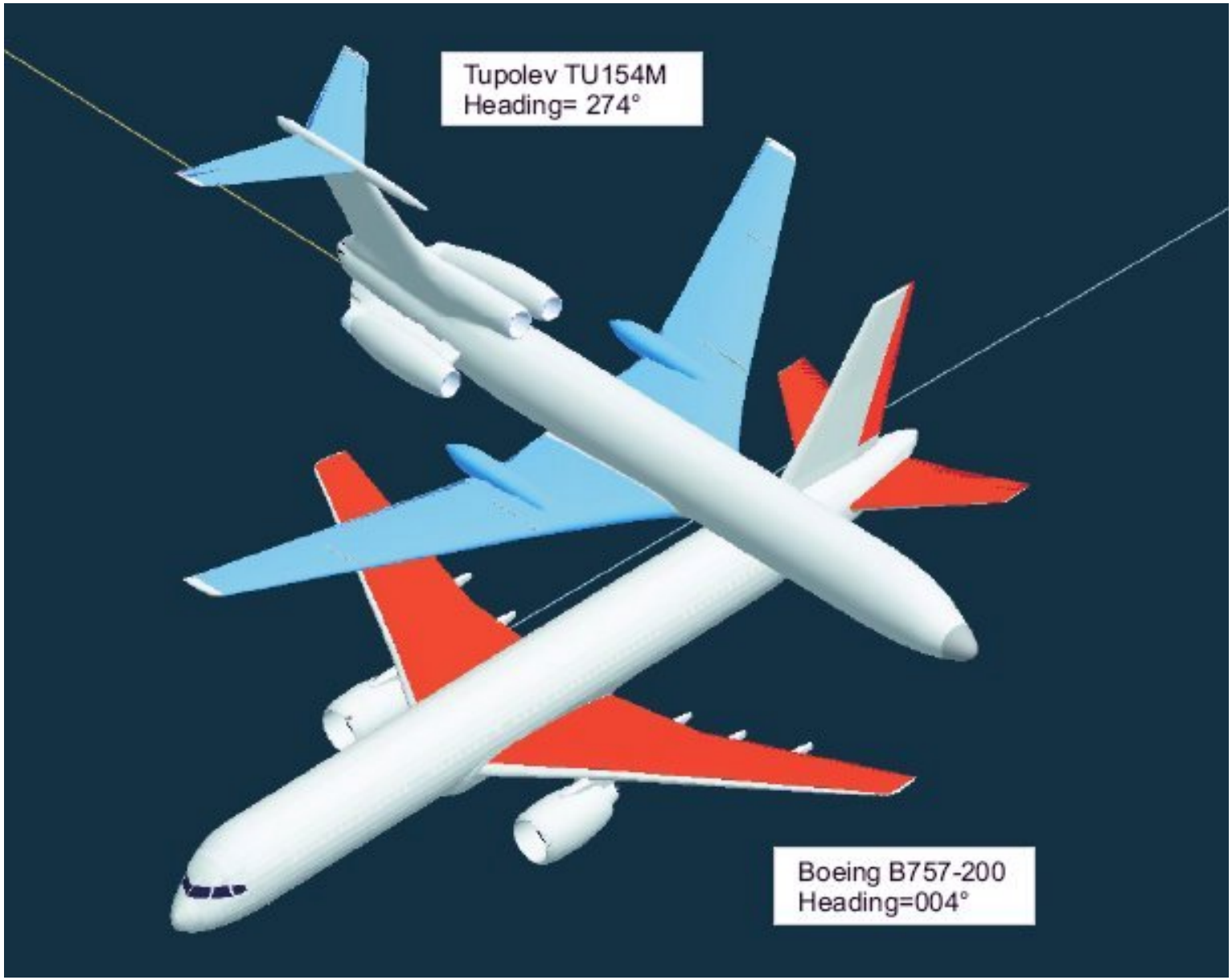
$+ x_2\omega\varpi\sin t\omega - u\omega\cos\vartheta\cos t\varpi\sin t\omega - u\omega\sqrt{1-\sin\vartheta^2}\sin t\omega$

$+ u\omega\cos\vartheta\cos t\omega\sin t\varpi + u\omega\sin\vartheta\sin t\omega\sin t\varpi\big)\ldots$

Mid-air Collision at Überlingen, Germany 2002

- Human at ATC detected conflict
- Human instructed Tupolev to descend
- TCAS instructed Tupolev to climb and Boeing to descend
- Boeing couldn't notify human (busy)
- Pilots on both aircraft descended
- Mid-air collision (less than a minute after conflict detected)

Mid-air Collision at Überlingen, Germany 2002



Hybrid Systems / Cyber-Physical Systems

Mathematical model for complex physical systems:

Definition (Hybrid Systems)

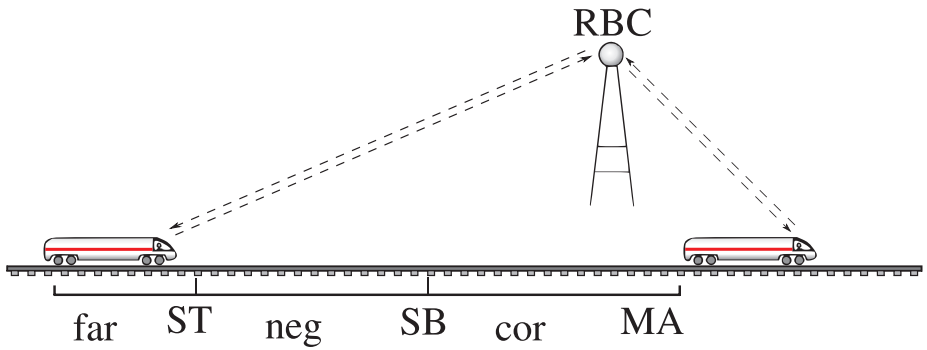
systems with interacting discrete and continuous dynamics

Technical characteristics:

Definition (Cyber-Physical Systems)

(Distributed network of) computerized control for physical system

European Train Control System



ETCS objectives:

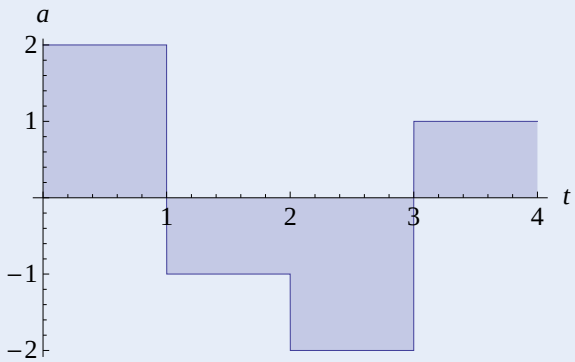
1. Collision free
2. Maximise throughput & velocity (320 km/h = 200 mph)
3. $2.1 * 10^6$ passengers/day

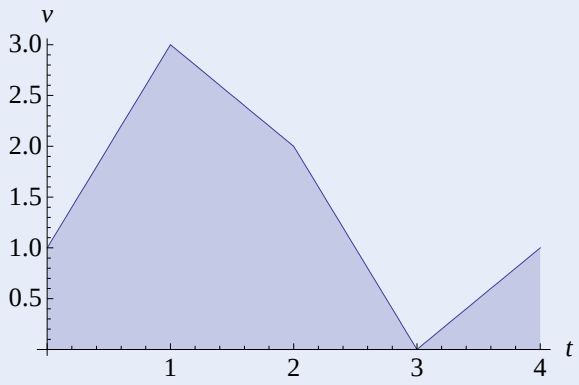
Train Control

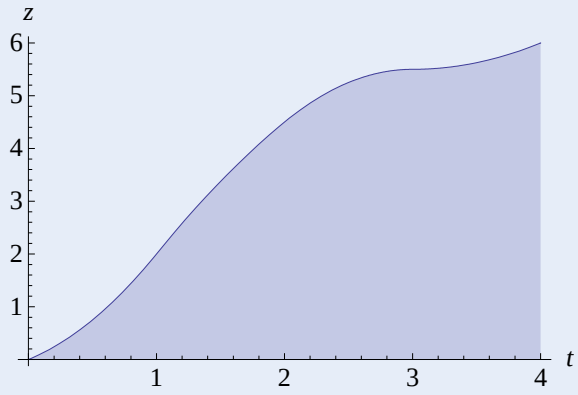
Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)





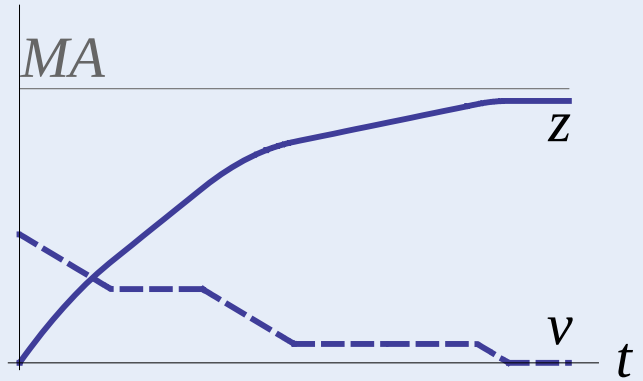


Train Control

Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

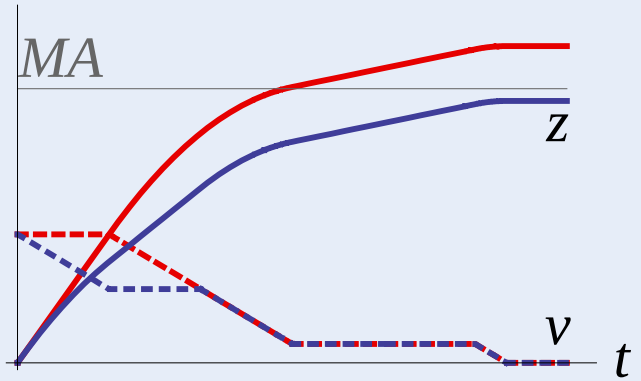


Train Control

Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

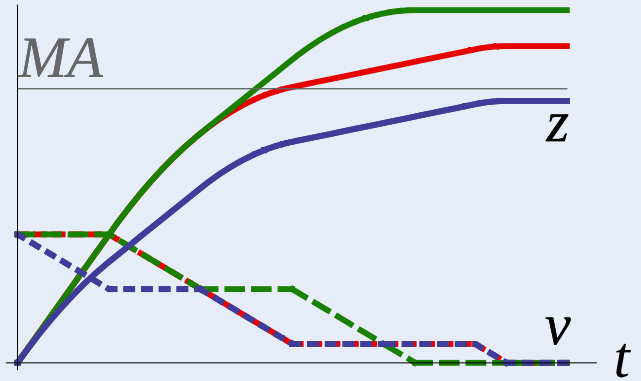


Train Control

Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



Train Control

Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

1. More than computers: no `NullPointerException` $\not\Rightarrow$ safe

Train Control

Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

1. More than computers: no `NullPointerException` $\not\Rightarrow$ safe
2. More than physics: braking control $v^2 \leq 2b(MA - z)$ $\not\Rightarrow$ safe

Train Control

Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

1. More than computers: no `NullPointerException` $\not\Rightarrow$ safe
2. More than physics: braking control $v^2 \leq 2b(MA - z) \not\Rightarrow$ safe
3. Joint dynamics requires:

$$SB \geq \frac{v^2}{2b} + \frac{a^2\varepsilon^2}{2b} + \frac{a}{b}\varepsilon v + \frac{a}{2}\varepsilon^2 + \varepsilon v \ldots$$

Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

Challenge

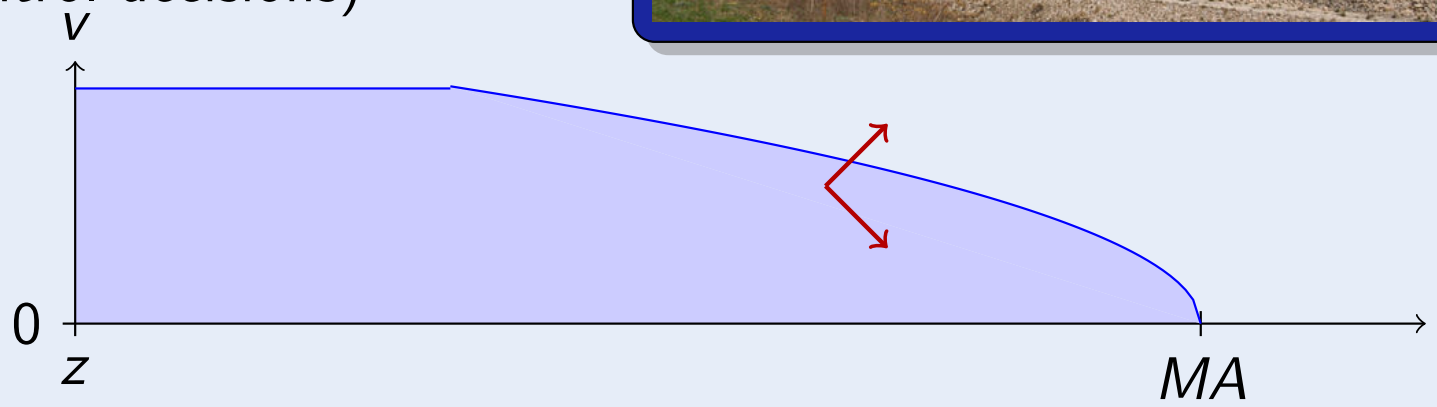
Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

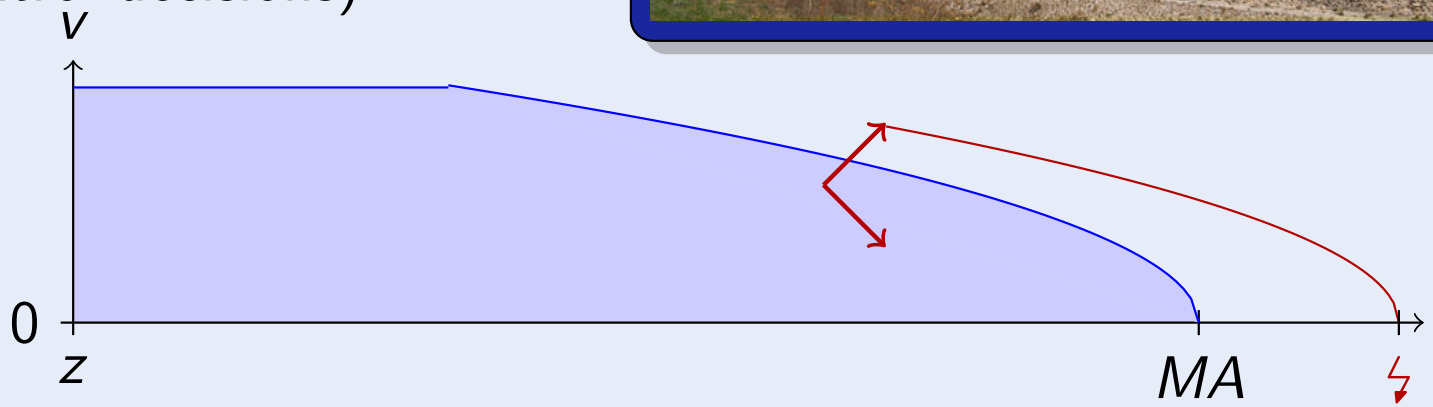


Train Control

Challenge

Hybrid systems

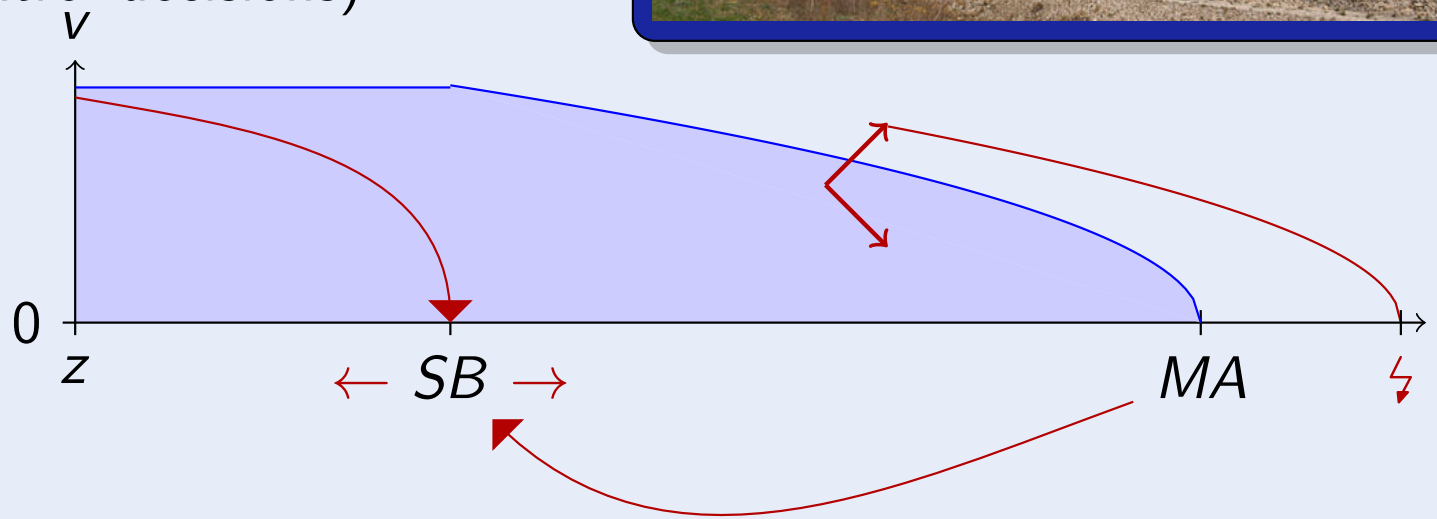
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



Challenge

Hybrid systems

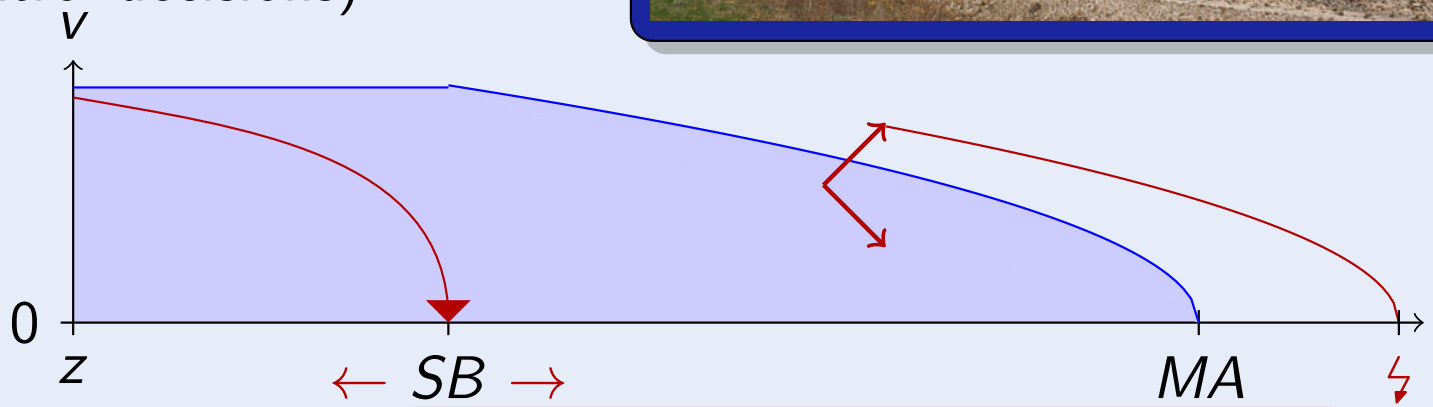
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

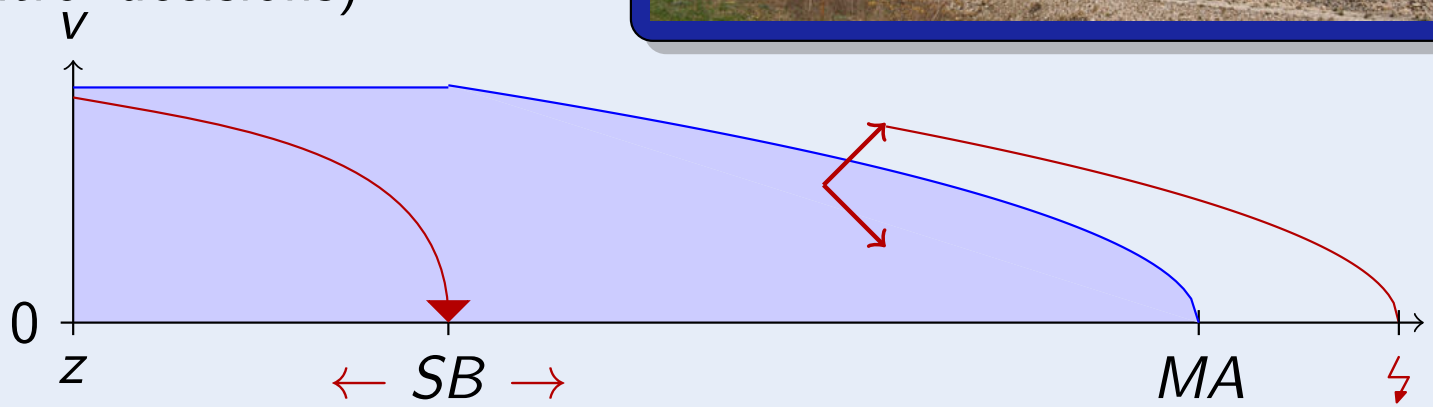


$$SB \geq \frac{v^2}{2b} + \frac{a^2\varepsilon^2}{2b} + \frac{a}{b}\varepsilon v + \frac{a}{2}\varepsilon^2 + \varepsilon v$$

Challenge

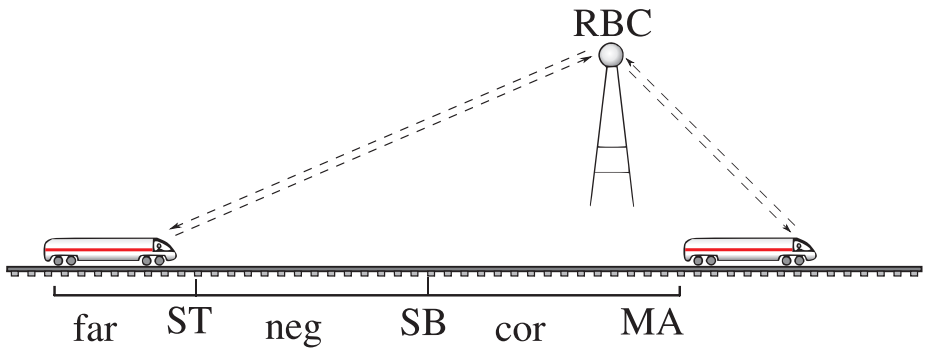
Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



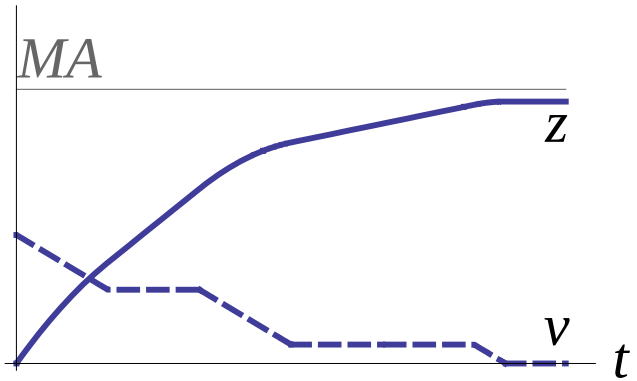
$\forall MA \exists SB$ "train always safe"

European Train Control System

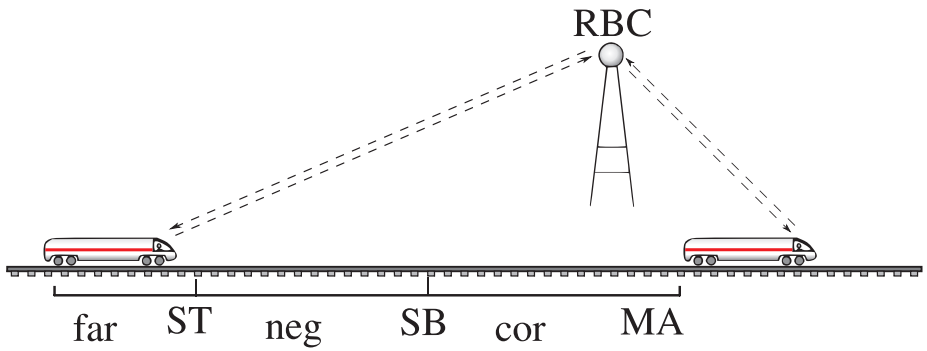


Parametric Hybrid Systems

continuous evolution along differential equations + discrete change

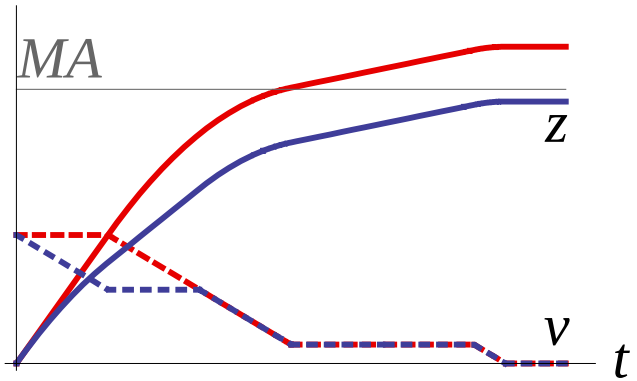


European Train Control System

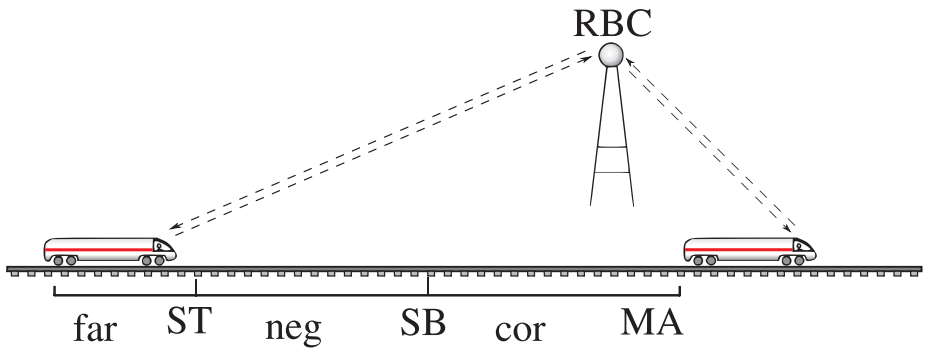


Parametric Hybrid Systems

continuous evolution along differential equations + discrete change

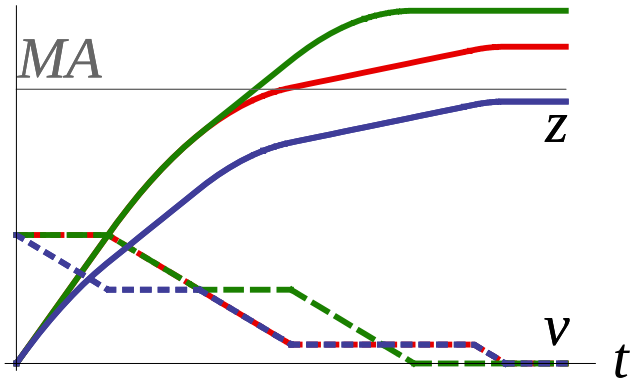


European Train Control System

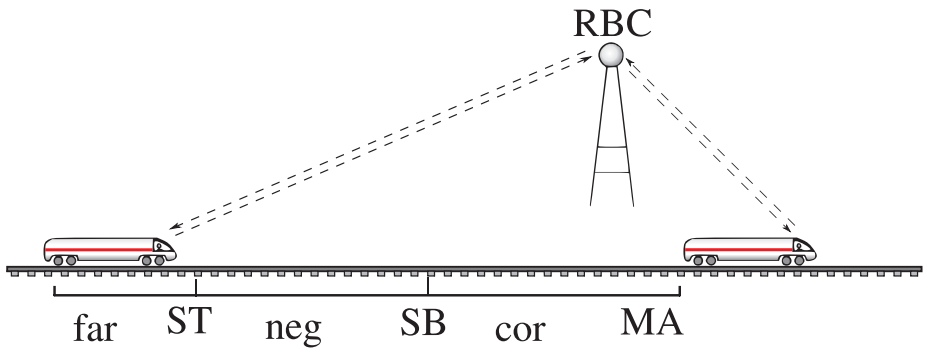


Parametric Hybrid Systems

continuous evolution along differential equations + discrete change



European Train Control System

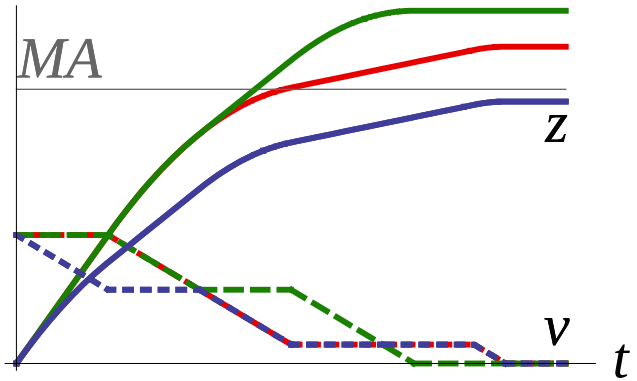


Parametric Hybrid Systems

continuous evolution along differential equations + discrete change

- Challenge: verification
- Which constraints for parameter SB?

$\forall MA \exists SB$ "train always safe"

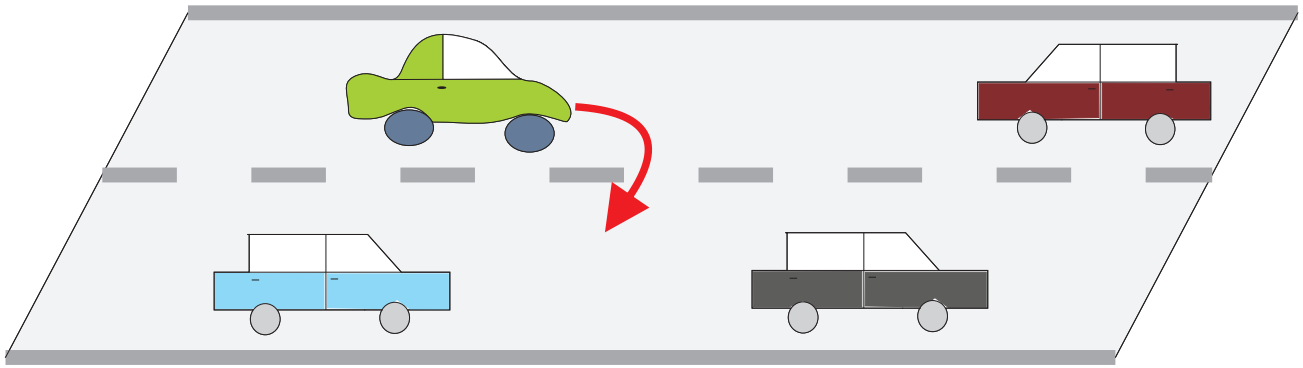


Head-on Train Collision at Chatsworth, CA 2008

- Train engineer disobeyed stop signal at single track section
- No warning issued to train dispatcher
- First sight 4 seconds before impact
- Freight train triggers emergency brakes 2 seconds before impact

Head-on Train Collision at Chatsworth, CA 2008

Car Control



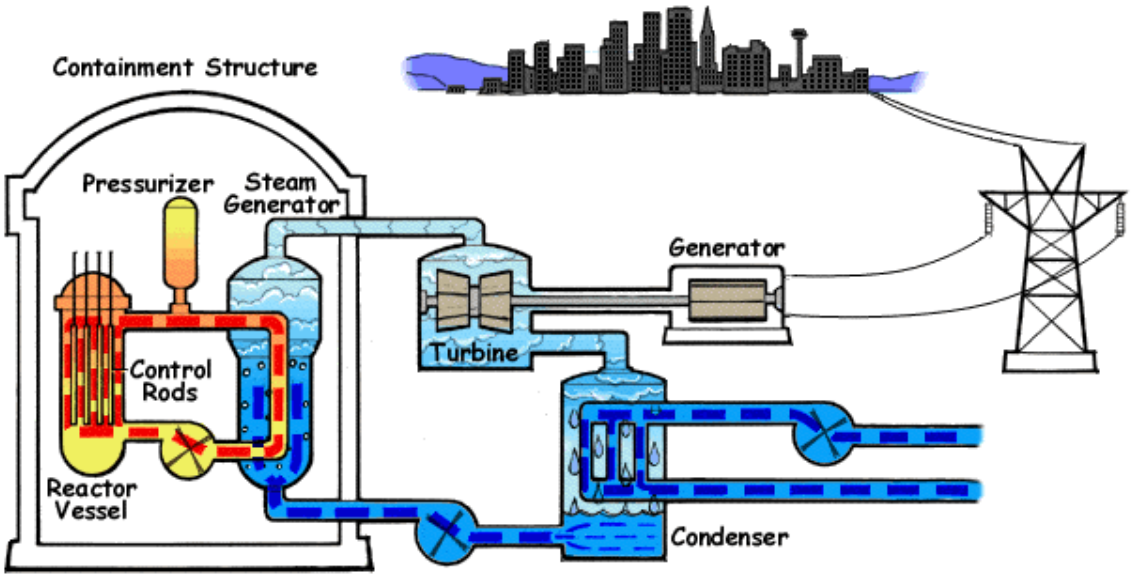
- Adaptive cruise control keeps safe distance?
- Lane change assistant
- Safe control with wireless interactions in CAR2CAR and USCAR
- Virtual car platooning

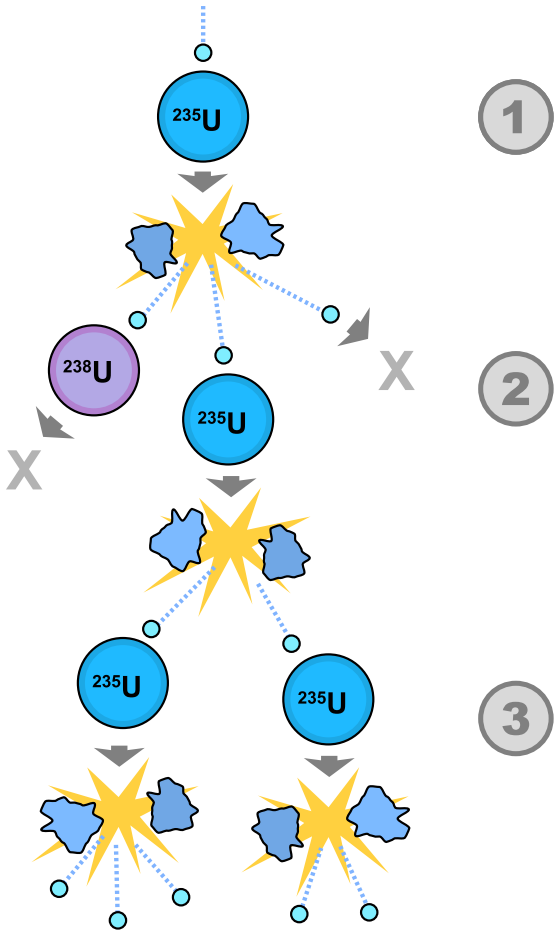
UAV - Unmanned Aerial Vehicle Control

UAV - Unmanned Aerial Vehicle Control

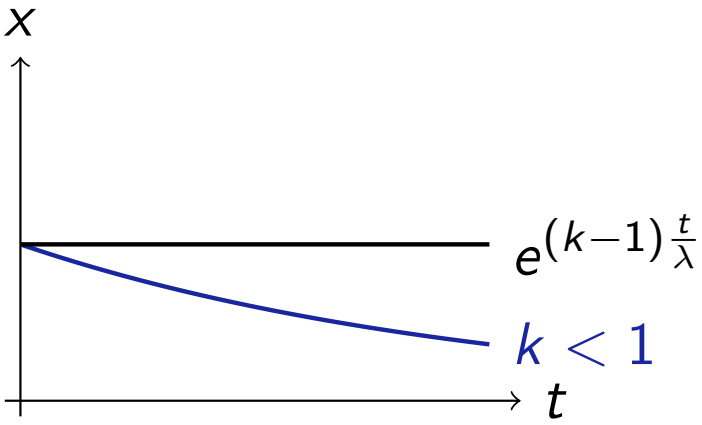
- Safe and stable UAV flight control
- Mixing UAV swarms into pilot flight control areas
- Refueling of UAV: mixed human operation and micro turbulences
- Many other robotic applications

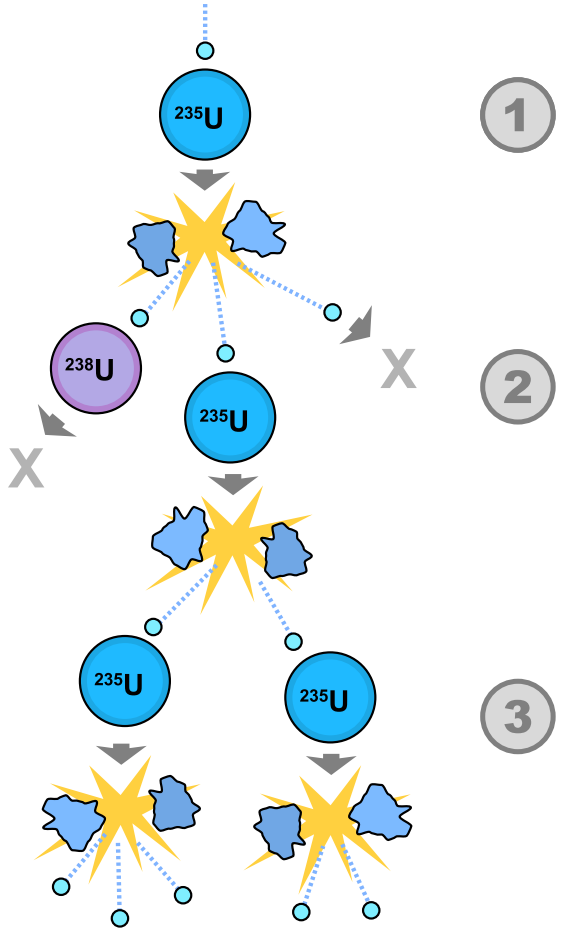
Computerized Chemical/Physical Process Control



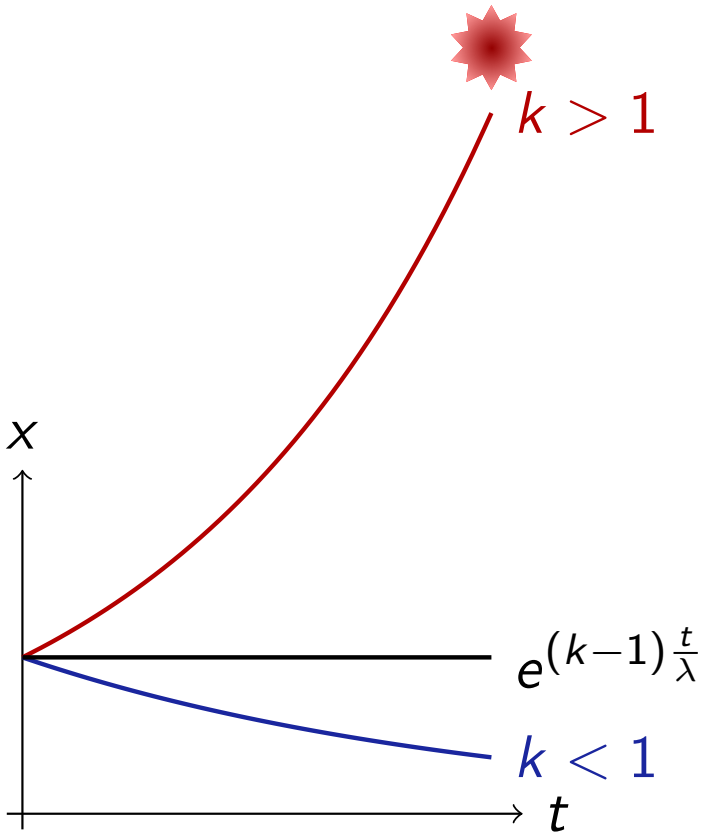


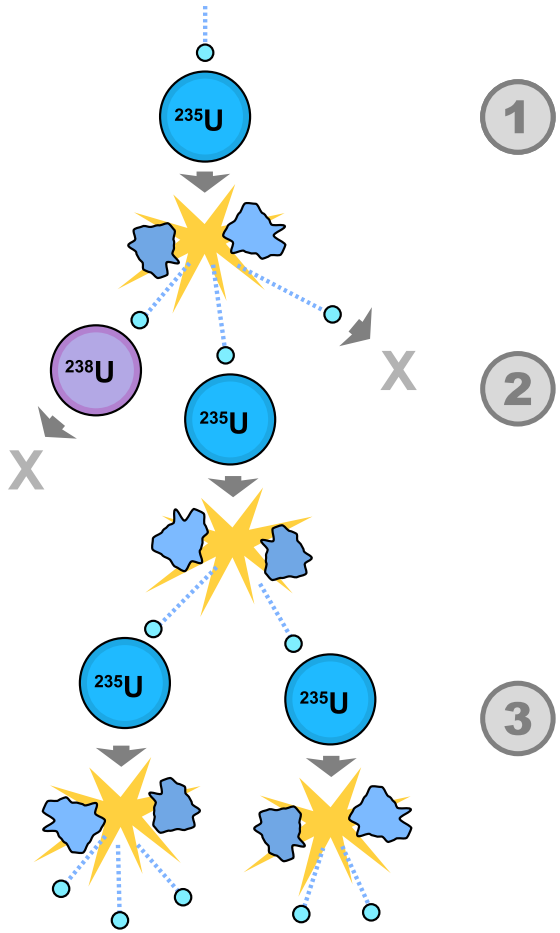
Computerized Chemical/Physical Process Control





Computerized Chemical/Physical Process Control

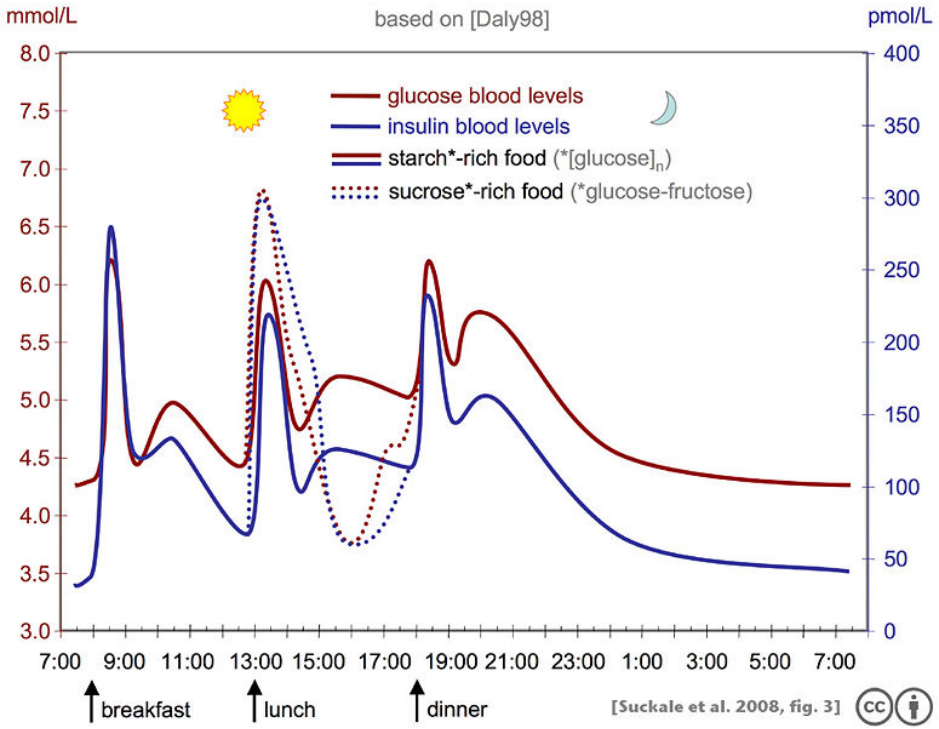




Control objective

Stabilize neutron multiplication factor

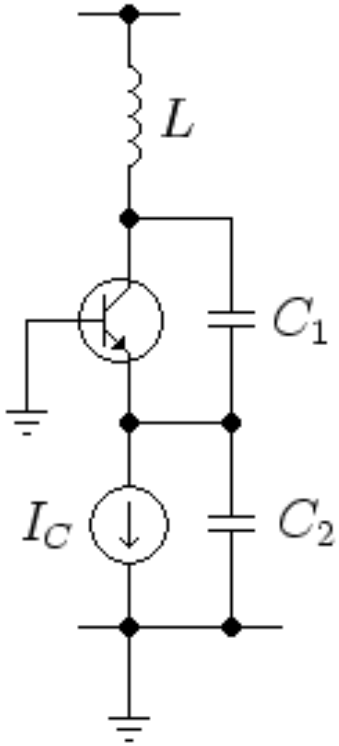
Biomedial Applications: Glucose/Insulin Regulation



Control objective

Maintain glucose in bounded range

Hybrid Effects in Chip Design



Hybrid Systems Analysis is Important for . . .