Model-bounded monitoring of hybrid systems

Masaki Waga[1], Étienne André[2], Ichiro Hasuo[3]

Kyoto University[1], Université de Lorraine[2],
National Institute of Informatics[3]

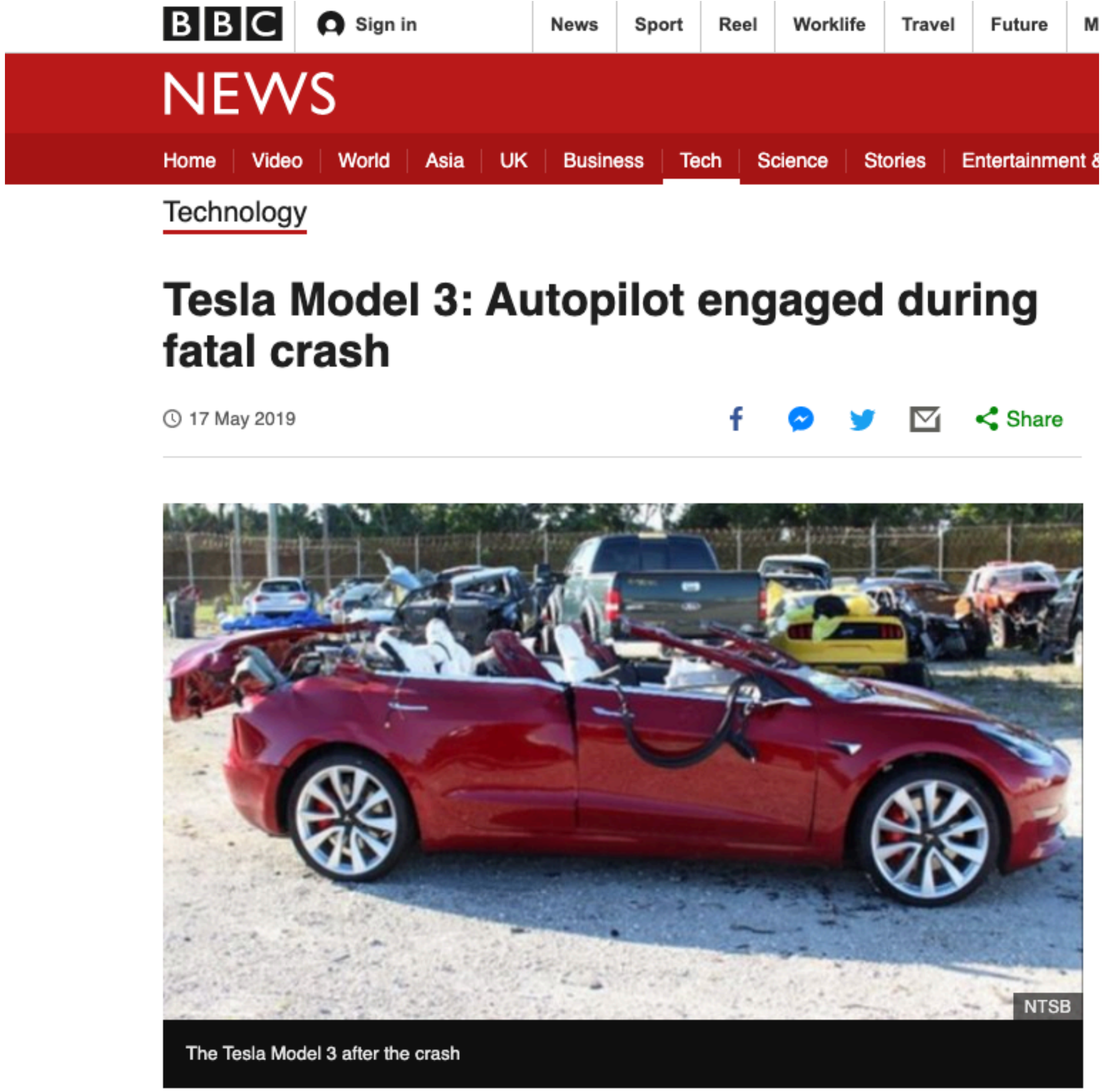
ICCPS 2021

This work is partially supported by JST ACT-X Grant No. JPMJAX200U, by JST ERATO HASUO Metamathematics for Systems Design Project (No. JPMJER1603), by JSPS Grant-in-Aid No. 18J22498, and by ANRNRF ProMiS (ANR-19-CE25-0015).

Safety Critical CPSs

Self-driving car crash in Arizona: Red light runner hits Waymo van

Copyright 2018 Scripps Media, Inc. All rights reserved. This material may not be published, broadcast, rewritten, or redistributed.
Photo by: Air15



Technology

Tesla Model 3: Autopilot engaged during fatal crash

17 May 2019

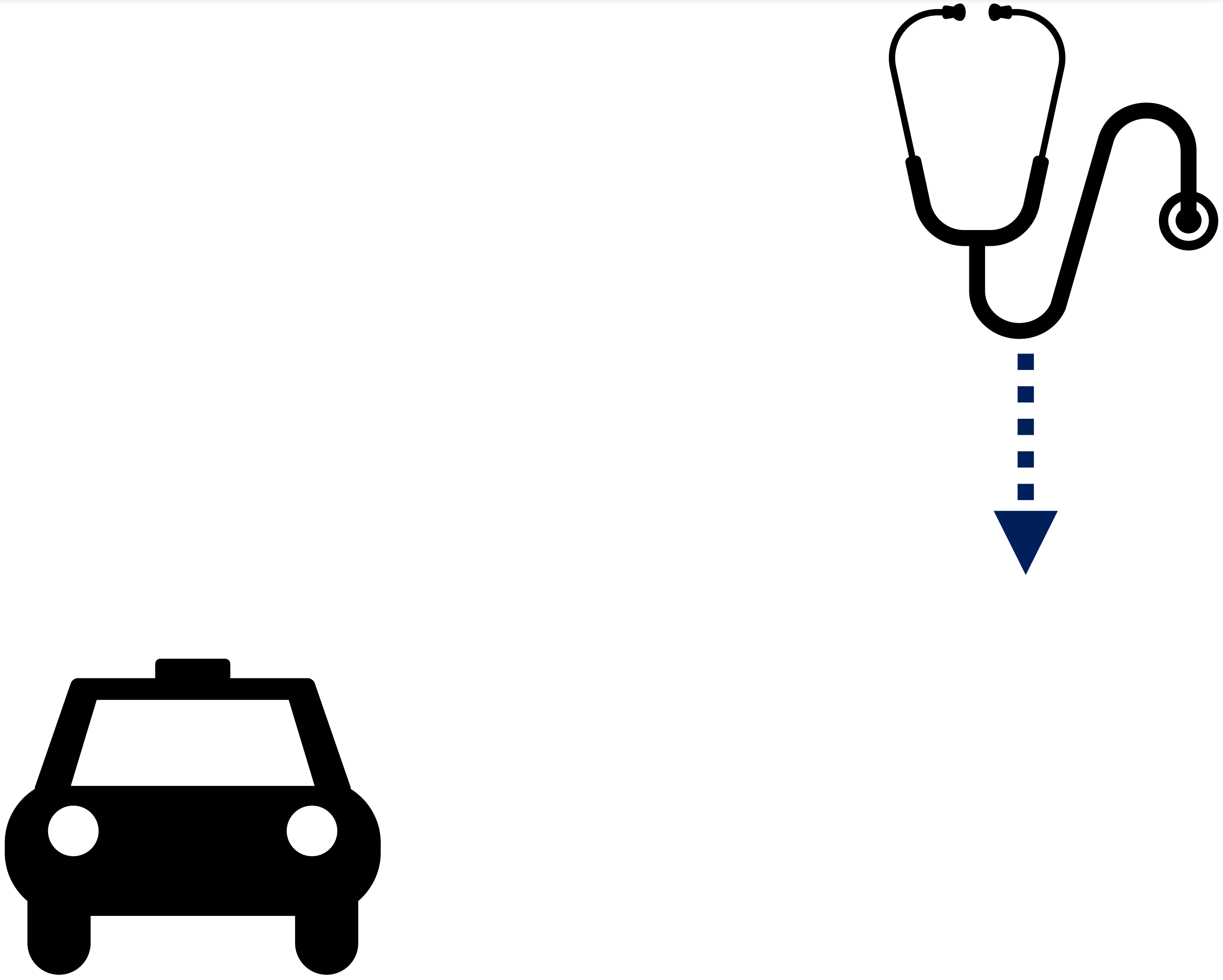
The Tesla Model 3 after the crash

https://www.abc15.com/news/region-southeast-valley/chandler/waymo-car-involved-in-chandler-arizona-crash

https://www.bbc.com/news/technology-48308852

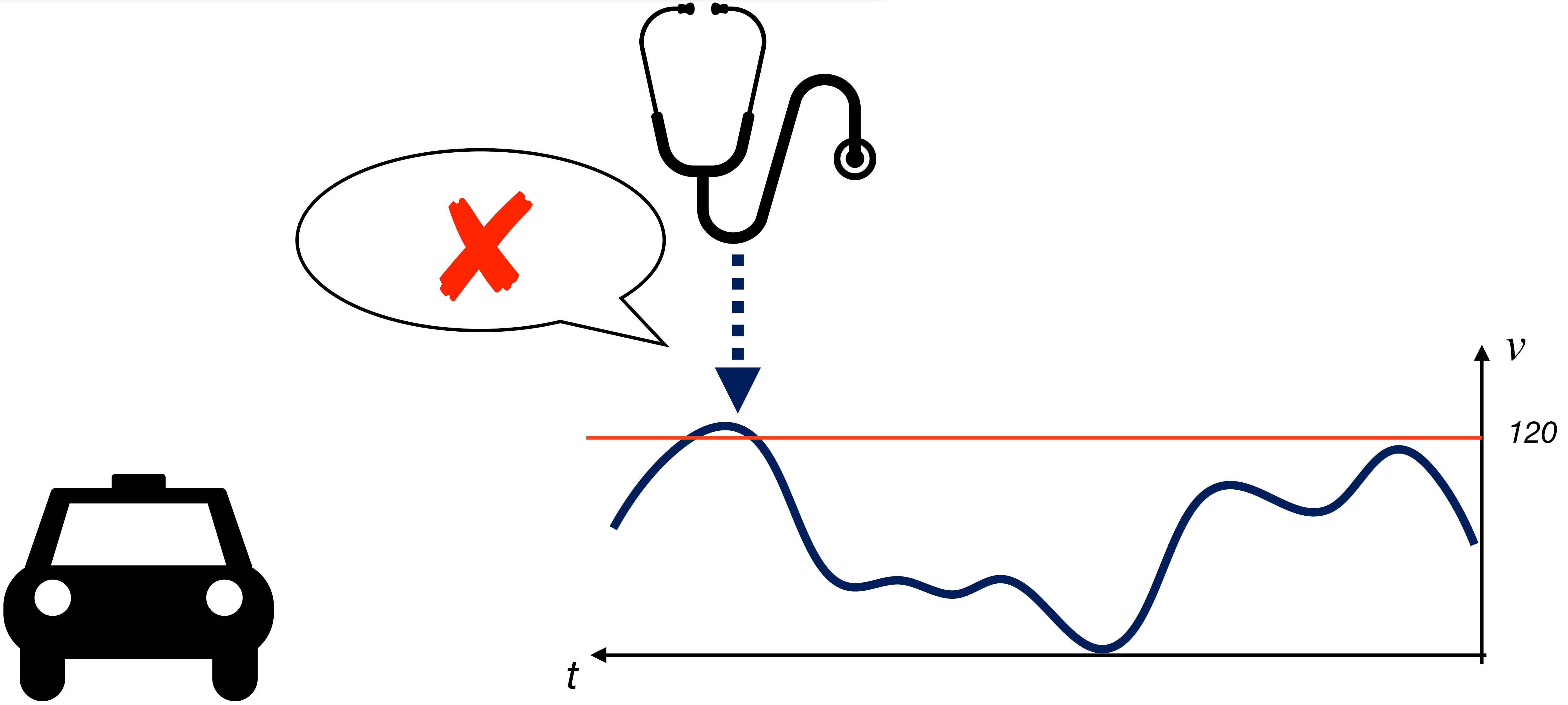
Monitoring

Specification: No $(v > 120)$



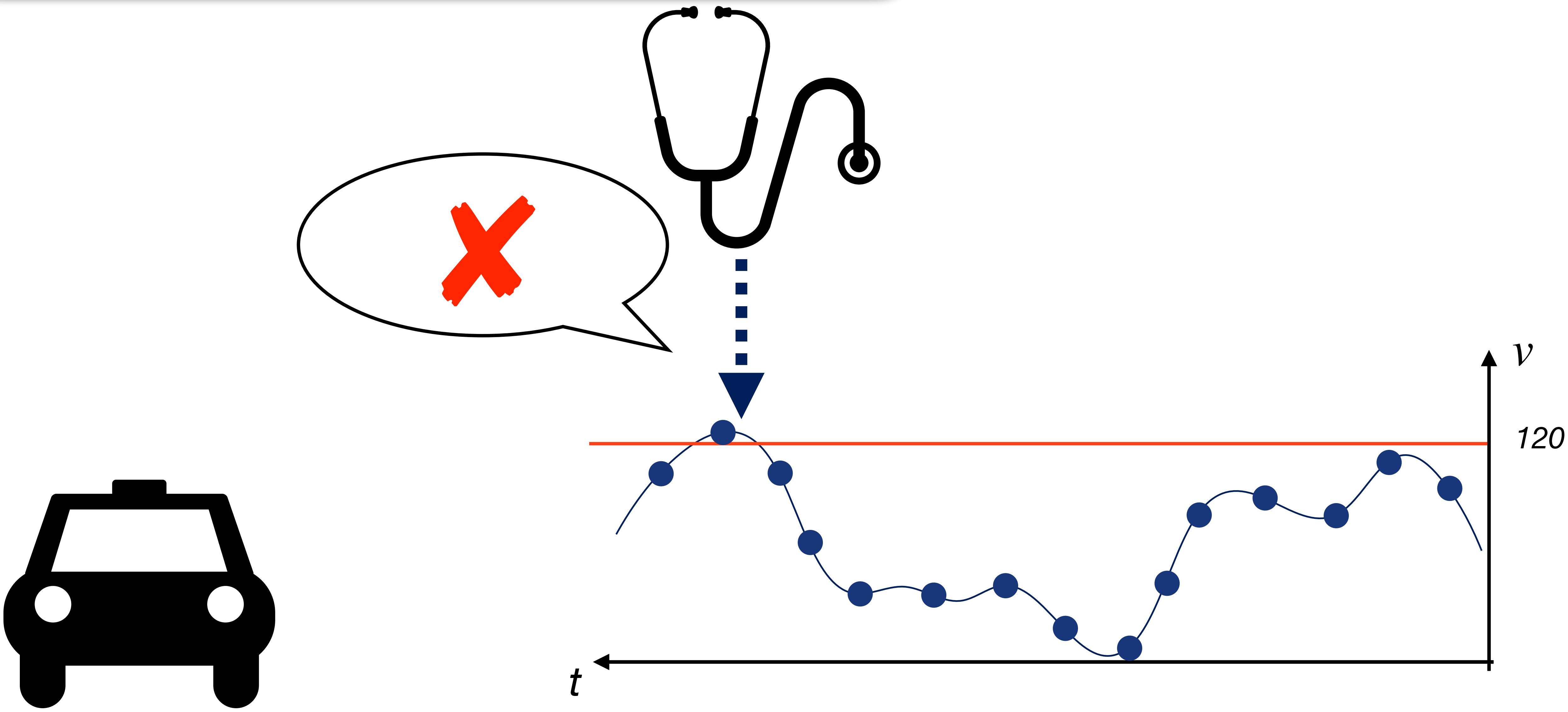
Monitoring

Specification: No $(v > 120)$



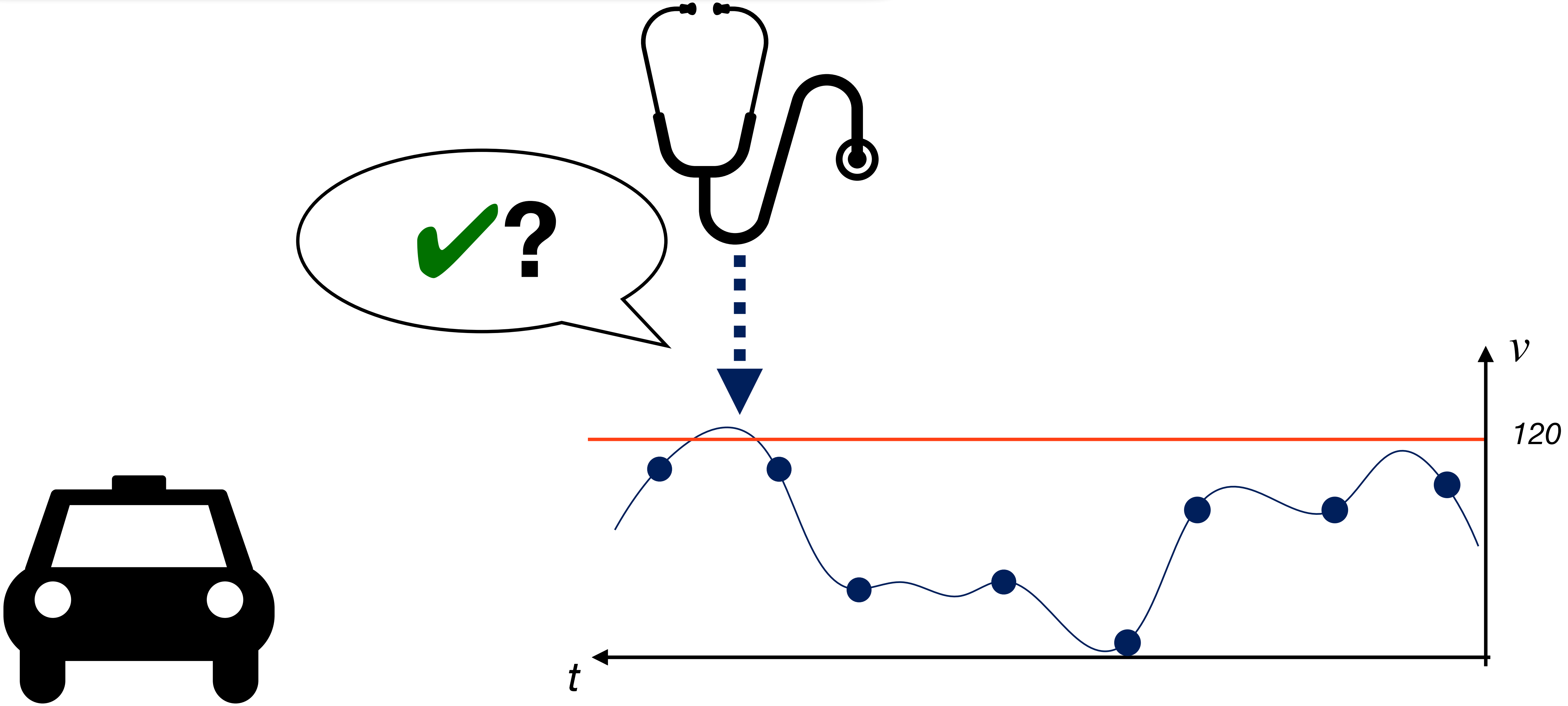
Monitoring with Sampling

Specification: No $(v > 120)$



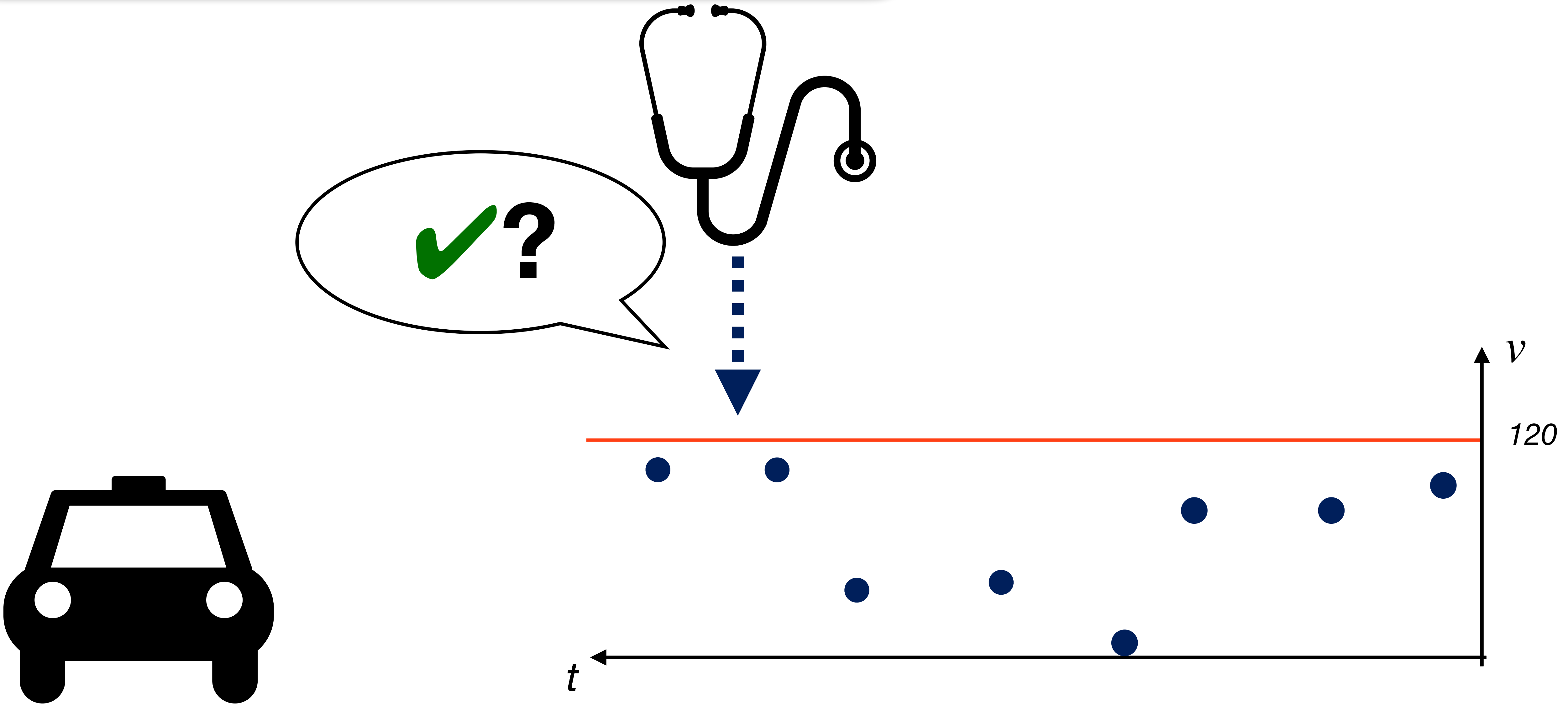
Monitoring with Sampling

Specification: No $(v > 120)$



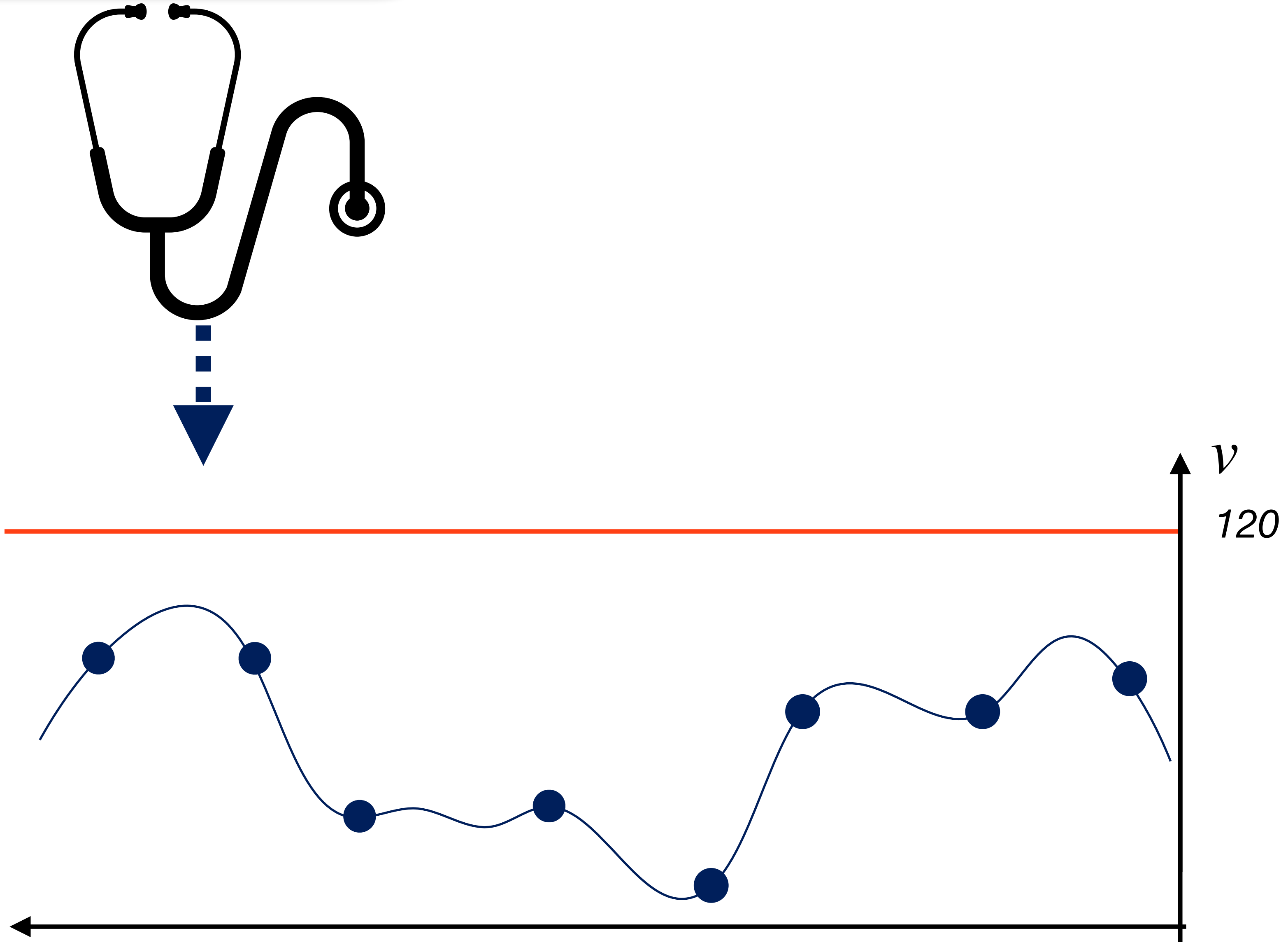
Monitoring with Sampling

Specification: No $(v > 120)$



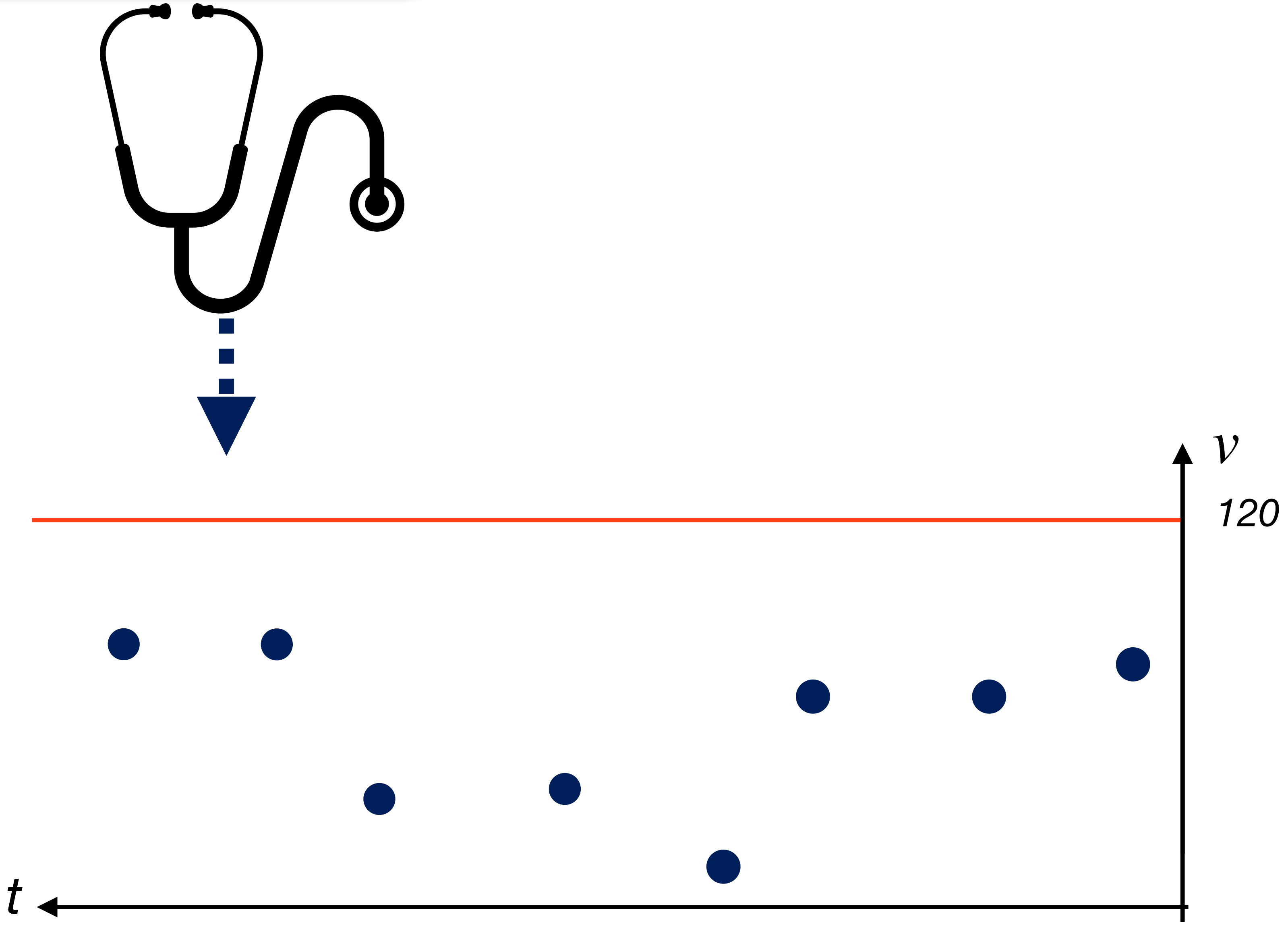
Signal Interpolation

Specification: **No** $(v > 120)$



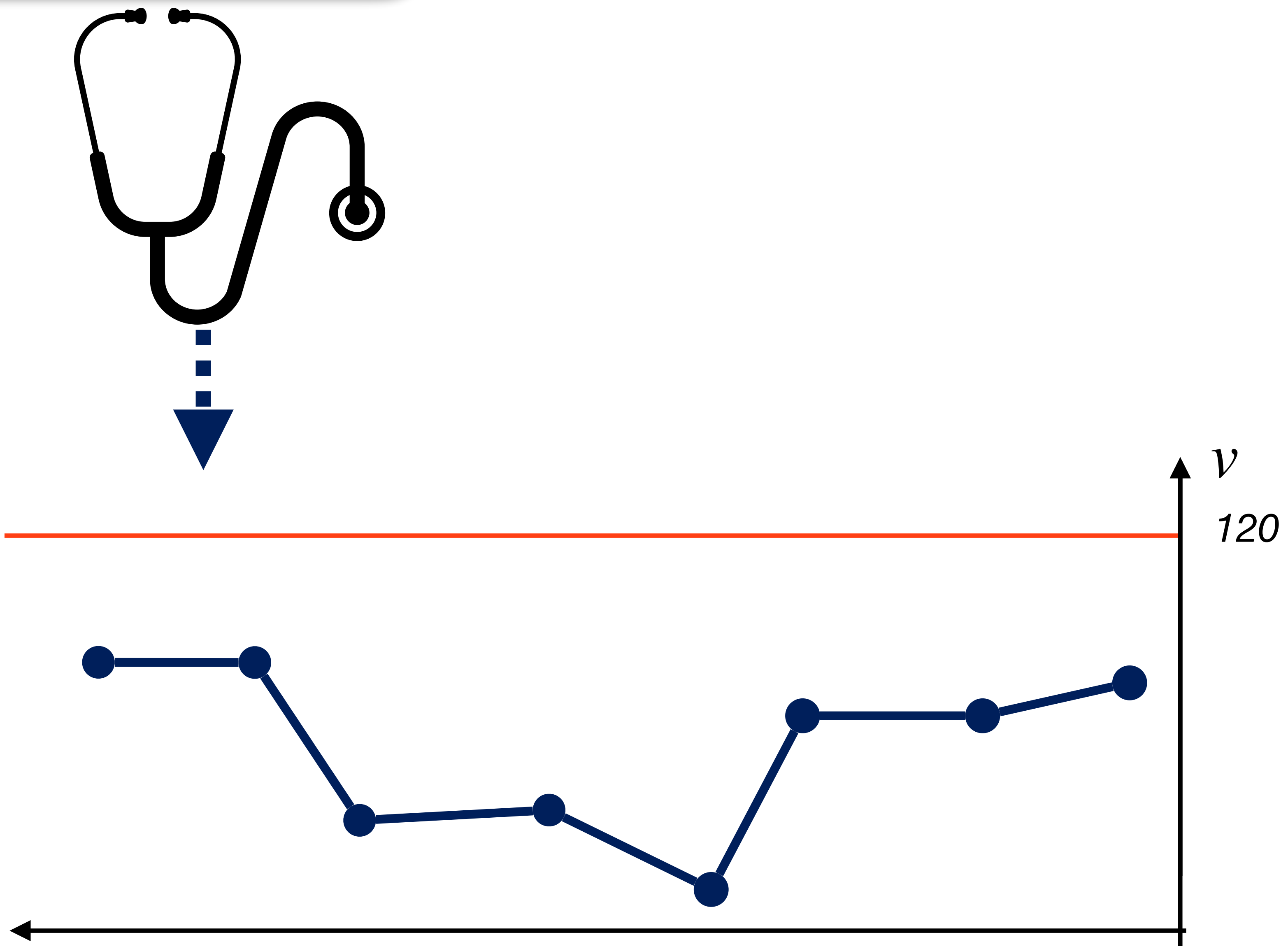
Signal Interpolation

Specification: **No** $(v > 120)$



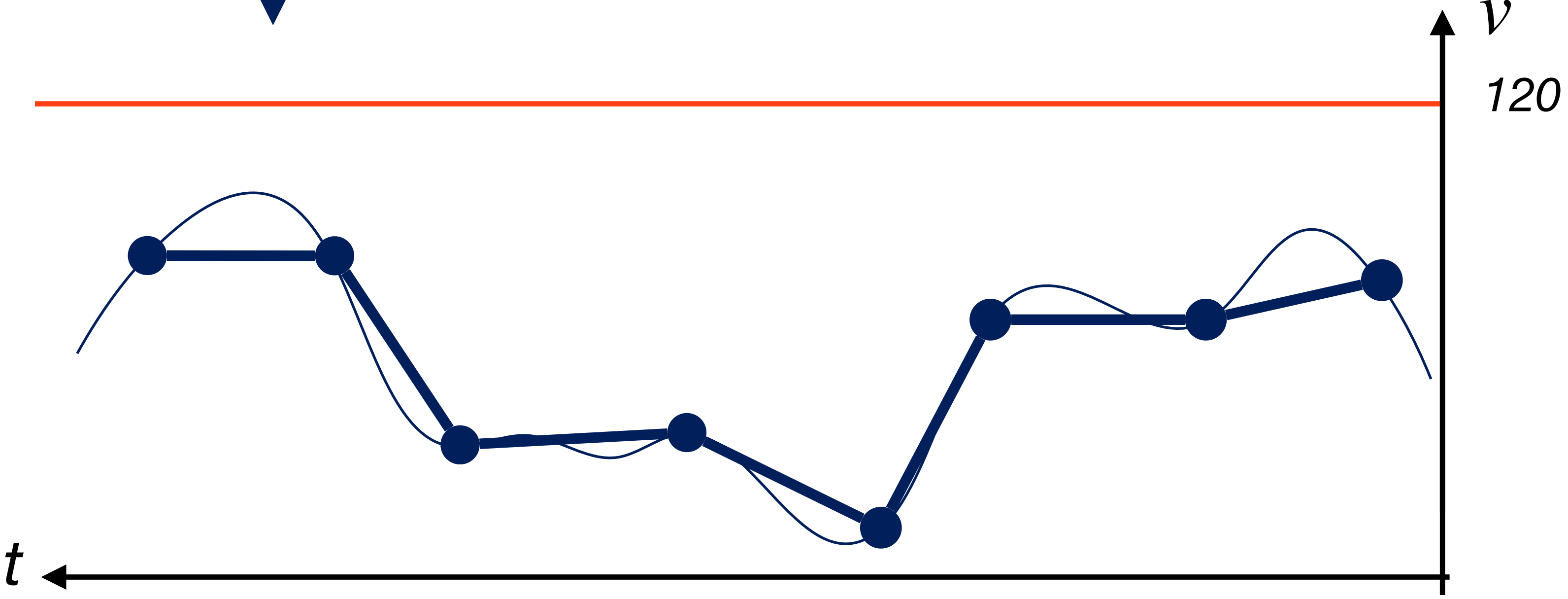
Signal Interpolation

Specification: No $(v > 120)$



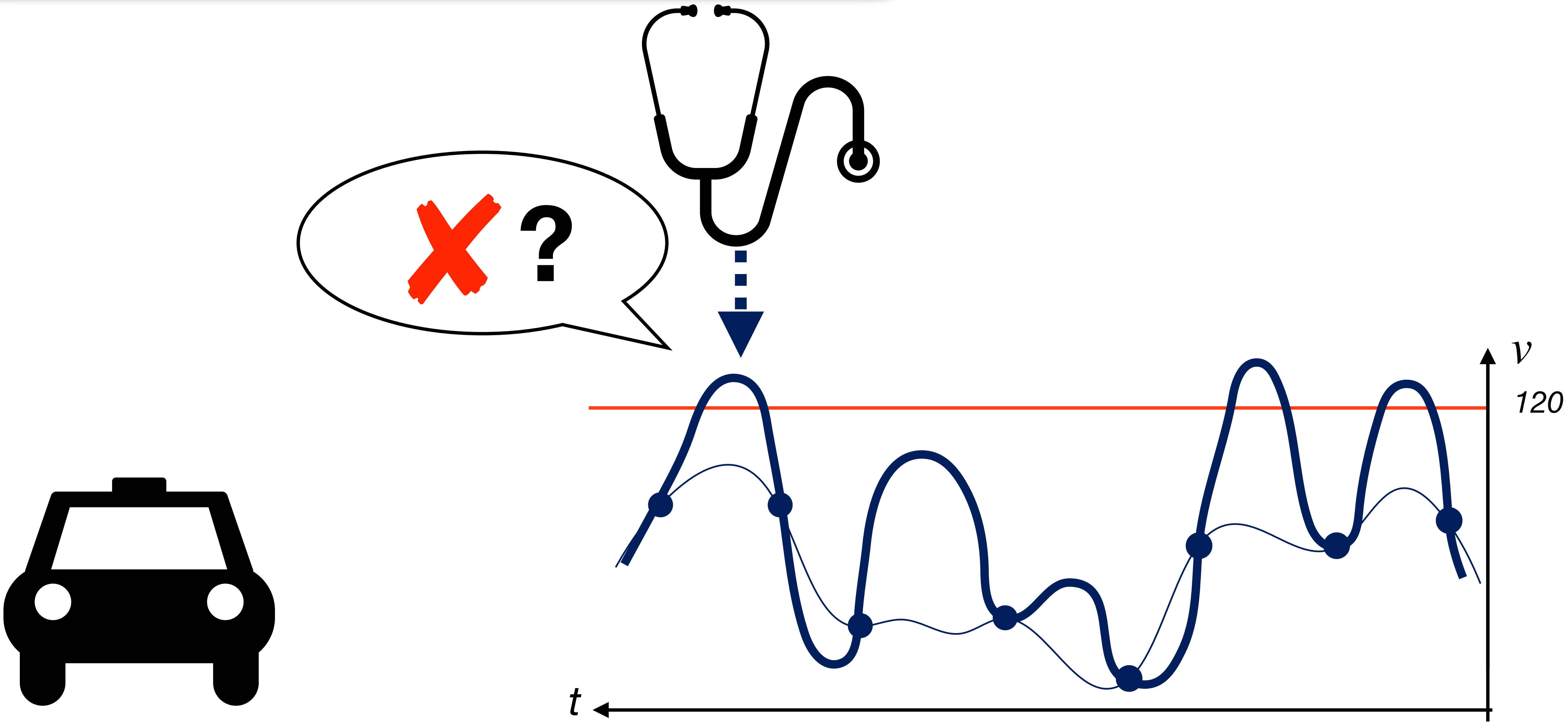
Signal Interpolation

Specification: No $(v > 120)$



Signal Interpolation

Specification: **No** $(v > 120)$

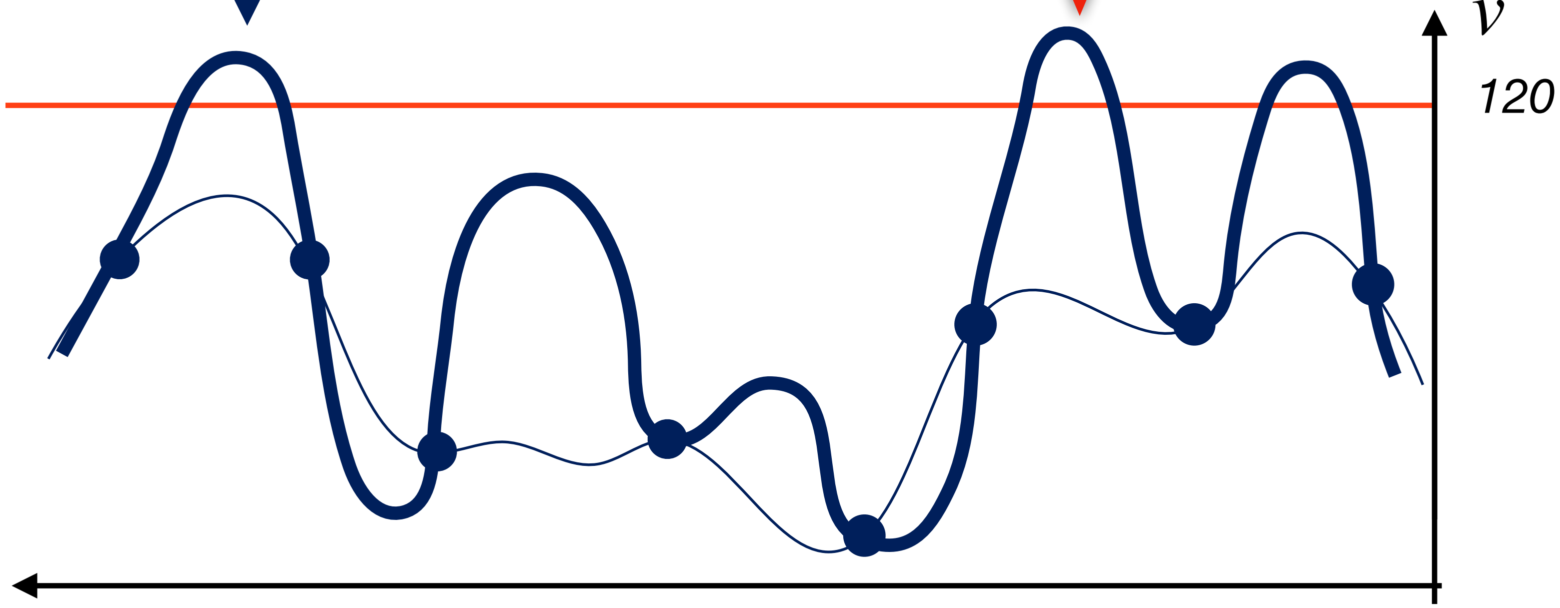


Interpolation with Prior Knowledge

Specification: No $(v > 120)$

Impossible because

$$\left|\frac{\mathrm{d}v}{\mathrm{d}t}\right| < K$$



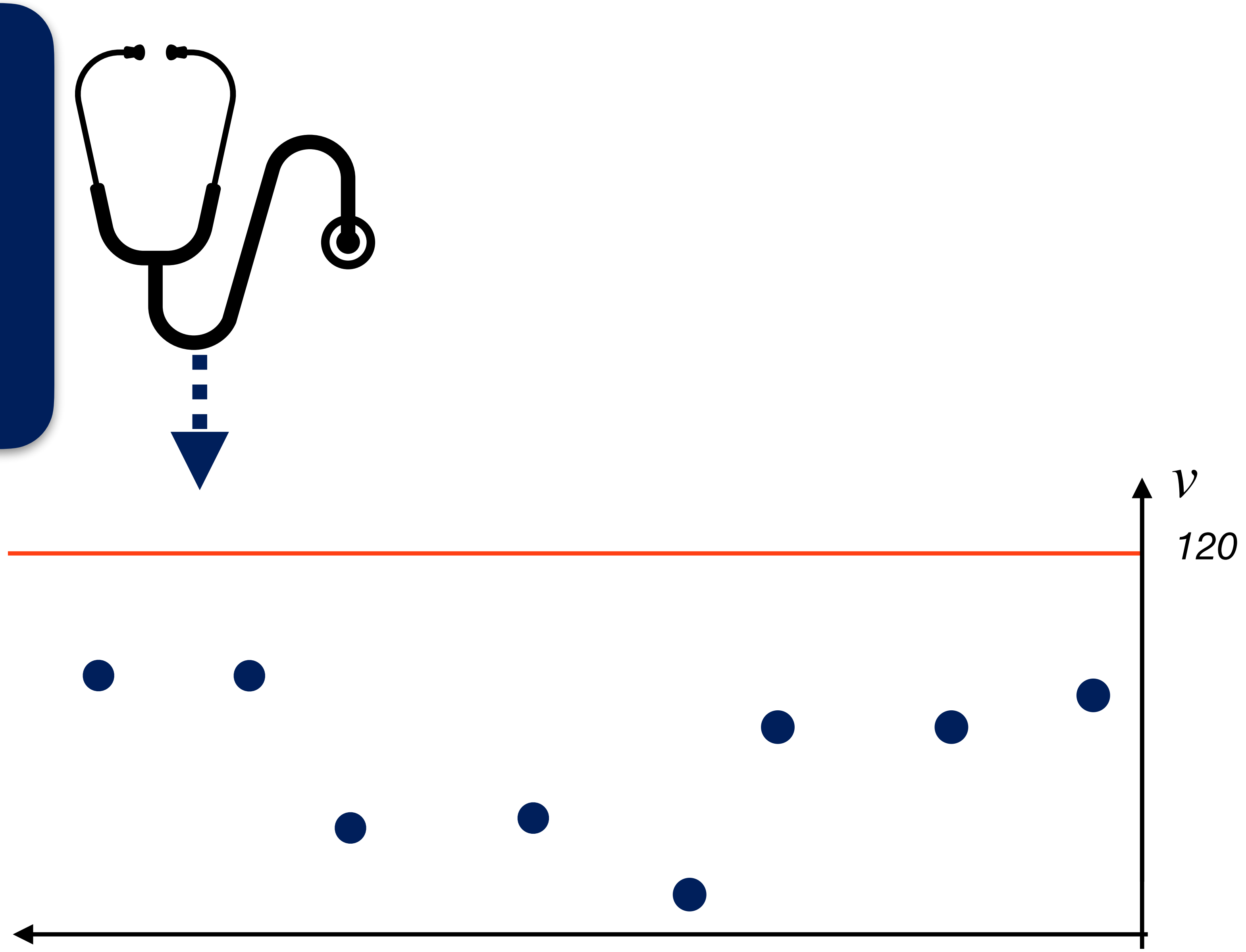
Model-Bounded Monitoring

Our Contribution

Specification: **No** $(v > 120)$

Knowledge (bounding model)

$$\left|\frac{\mathrm{d}v}{\mathrm{d}t}\right| < K$$



Model-Bounded Monitoring

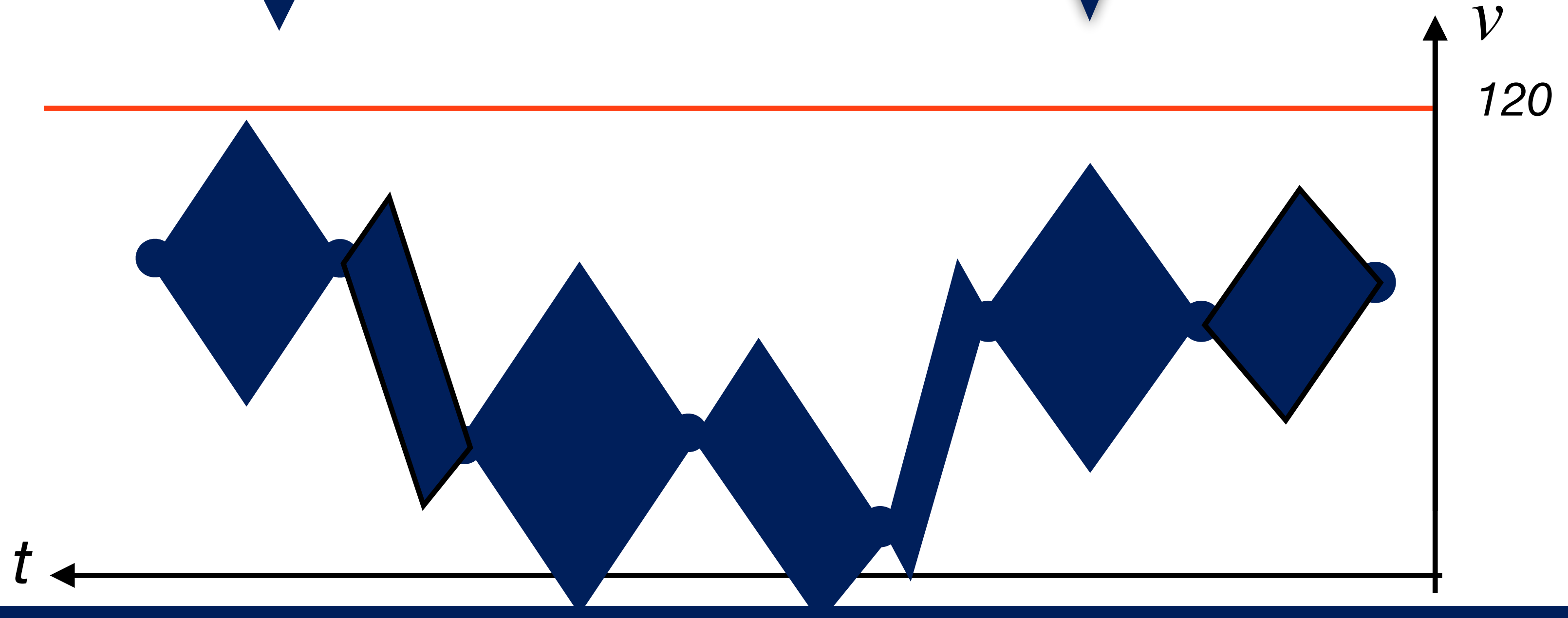
Our Contribution

Specification: No $(v > 120)$

Knowledge (bounding model)

$$\left|\frac{\mathrm{d}v}{\mathrm{d}t}\right| < K$$

Feasible execution with $\left|\frac{\mathrm{d}v}{\mathrm{d}t}\right| < K$



Model-Bounded Monitoring

Our Contribution

Specification: No $(v > 120)$

Knowledge (bounding model)

$$\left|\frac{\mathrm{d}v}{\mathrm{d}t}\right| < K$$

Model-Bounded Monitoring

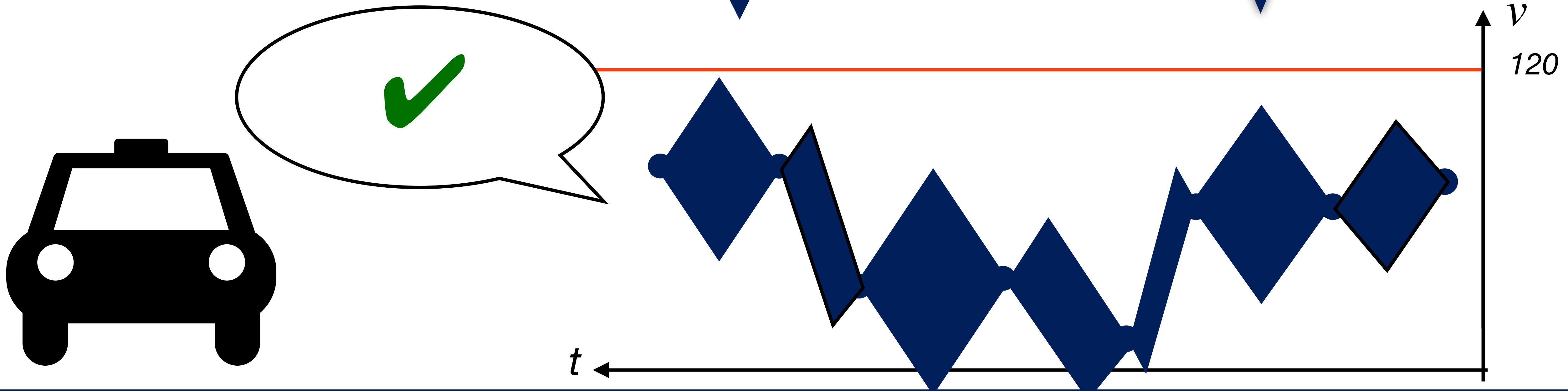
Our Contribution

Specification: No $(v > 120)$

Knowledge (bounding model)

$$\left|\frac{\mathrm{d}v}{\mathrm{d}t}\right| < K$$

Feasible execution with $\left|\frac{\mathrm{d}v}{\mathrm{d}t}\right| < K$

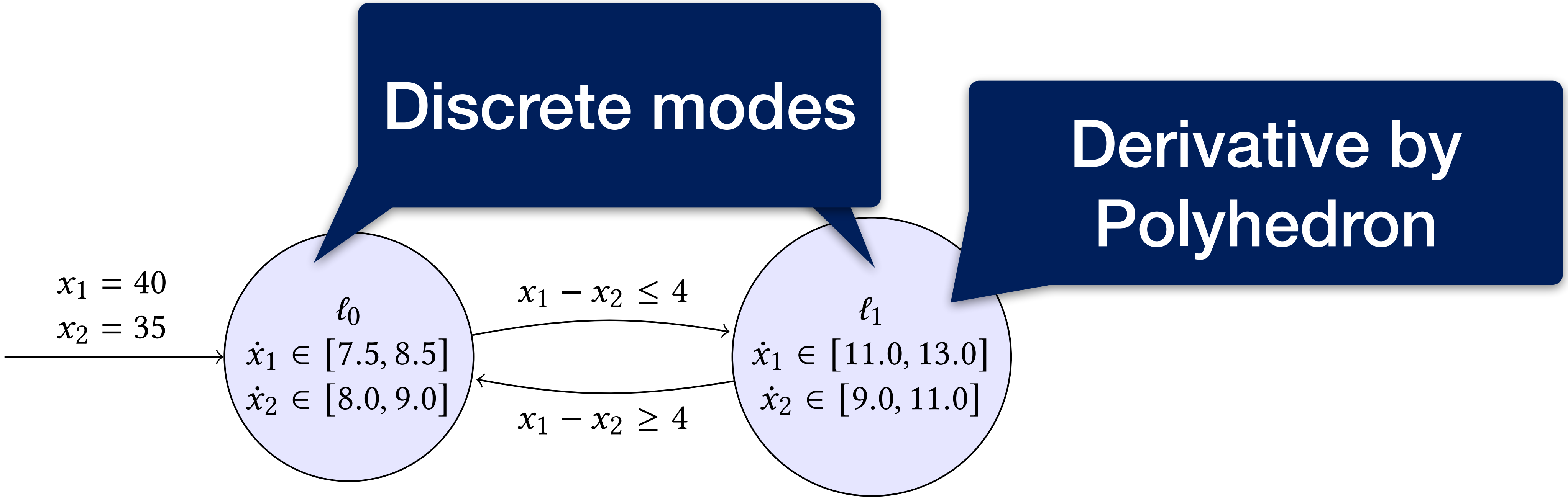


Q. How to Represent Bounding Model?

Knowledge (bounding model)

$$\left|\frac{\mathrm{d}v}{\mathrm{d}t}\right| < K$$

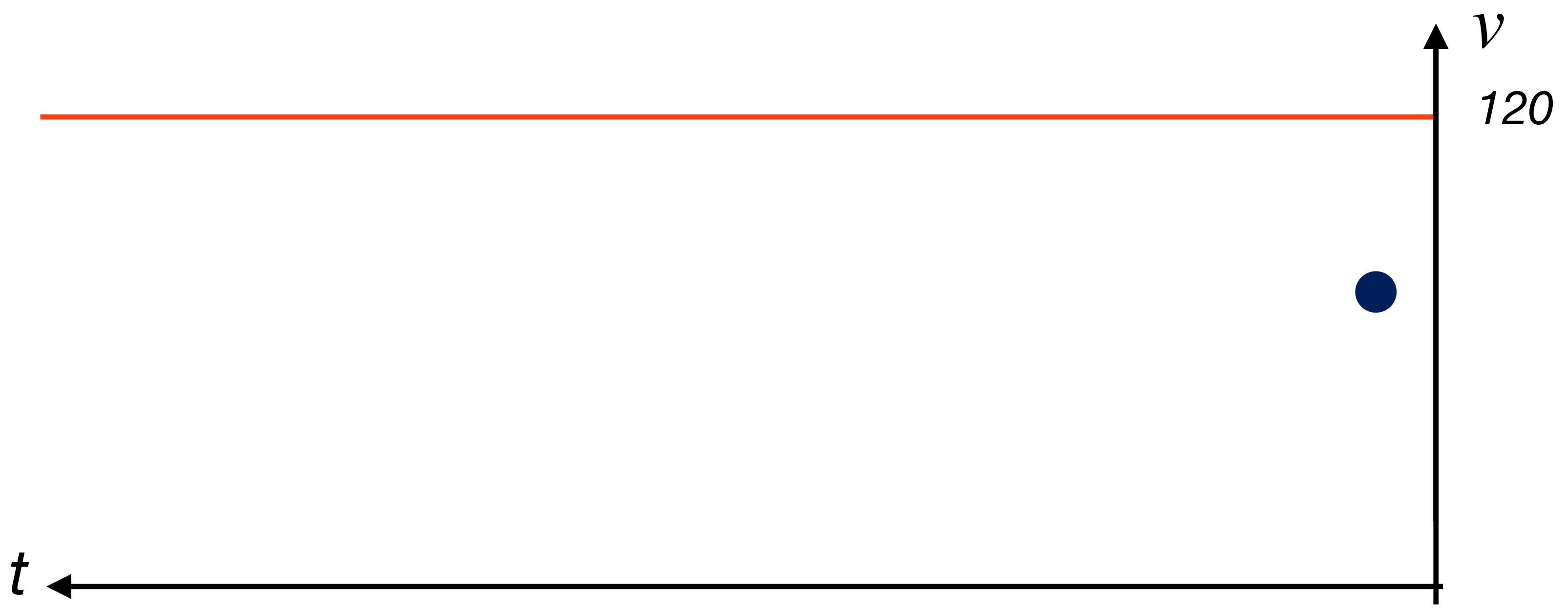
A. Linear Hybrid Automata


Discrete modes

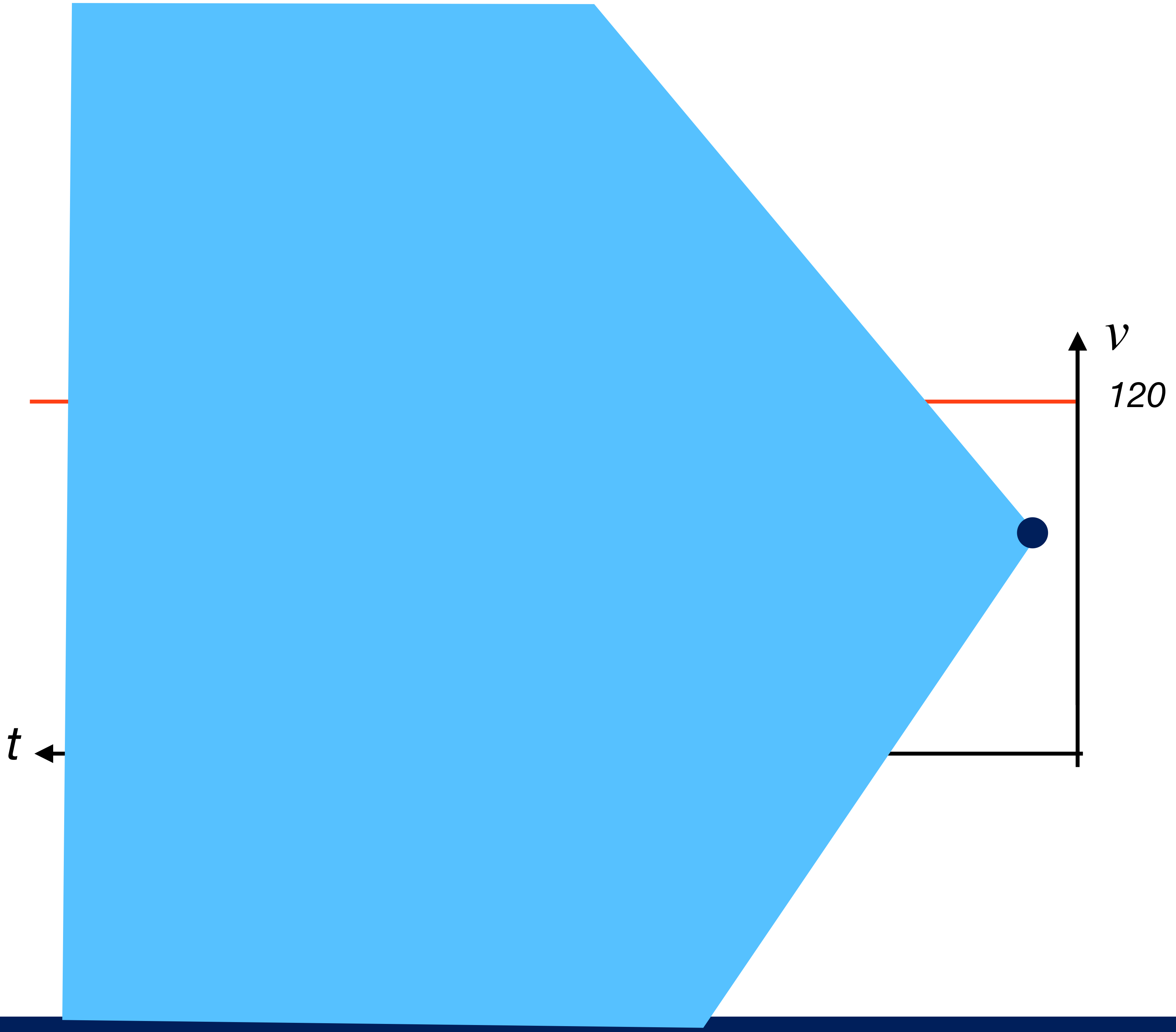
Derivative by Polyhedron

$x_1 = 40$
$x_2 = 35$
ℓ_0
$\dot{x}_1 \in [7.5, 8.5]$
$\dot{x}_2 \in [8.0, 9.0]$
$x_1 - x_2 \leq 4$
$x_1 - x_2 \geq 4$
ℓ_1
$\dot{x}_1 \in [11.0, 13.0]$
$\dot{x}_2 \in [9.0, 11.0]$

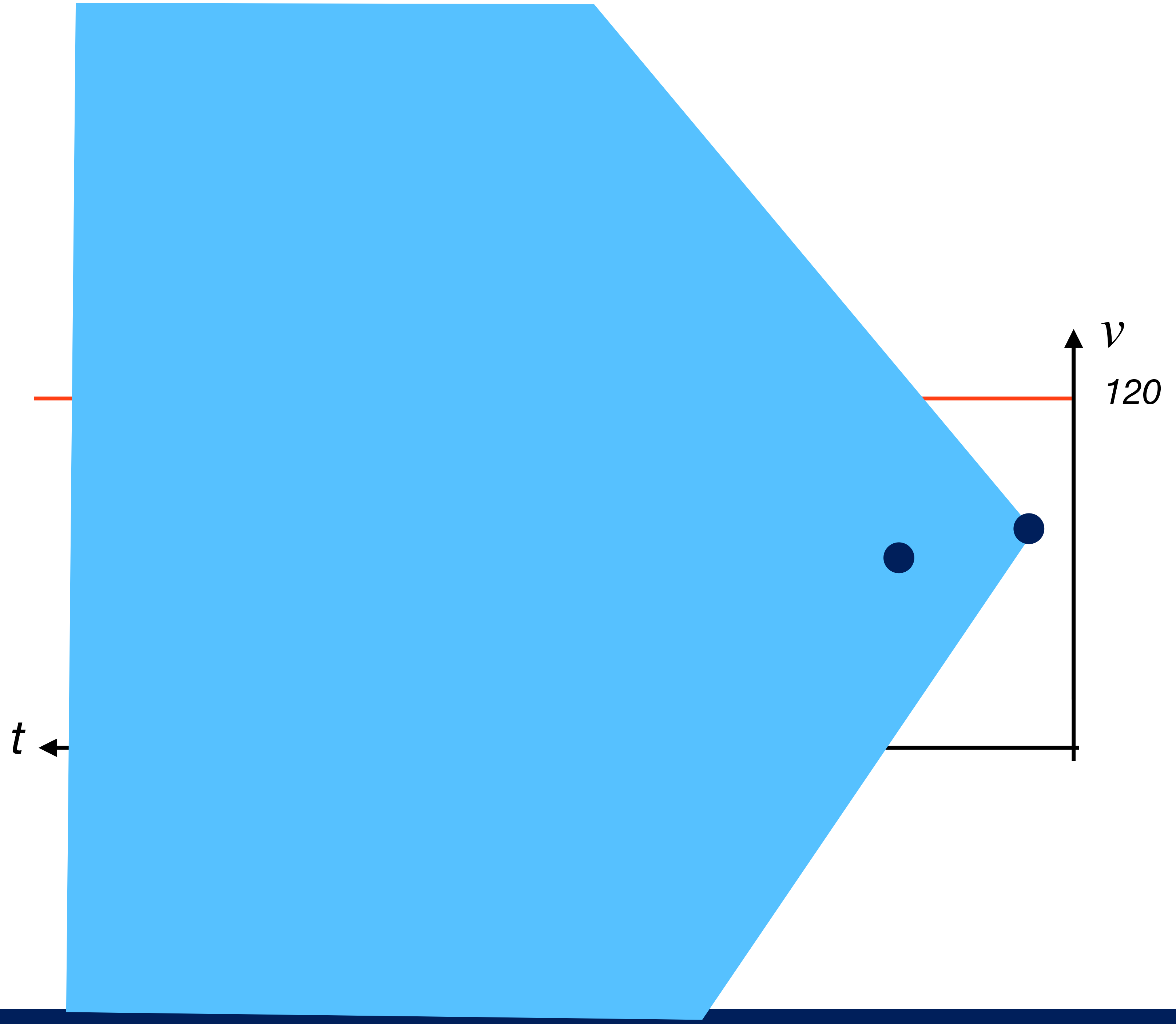
Algorithm: Bounded-time Reachability



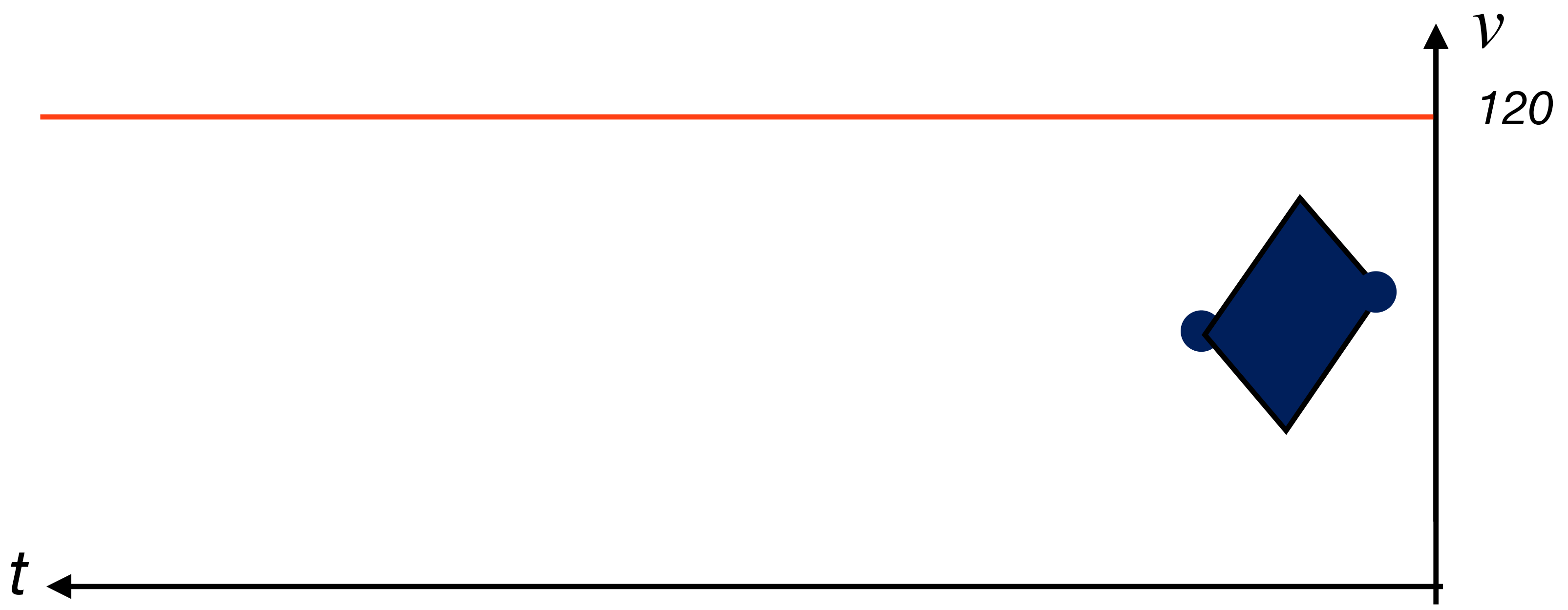
Algorithm:
Bounded-time Reachability



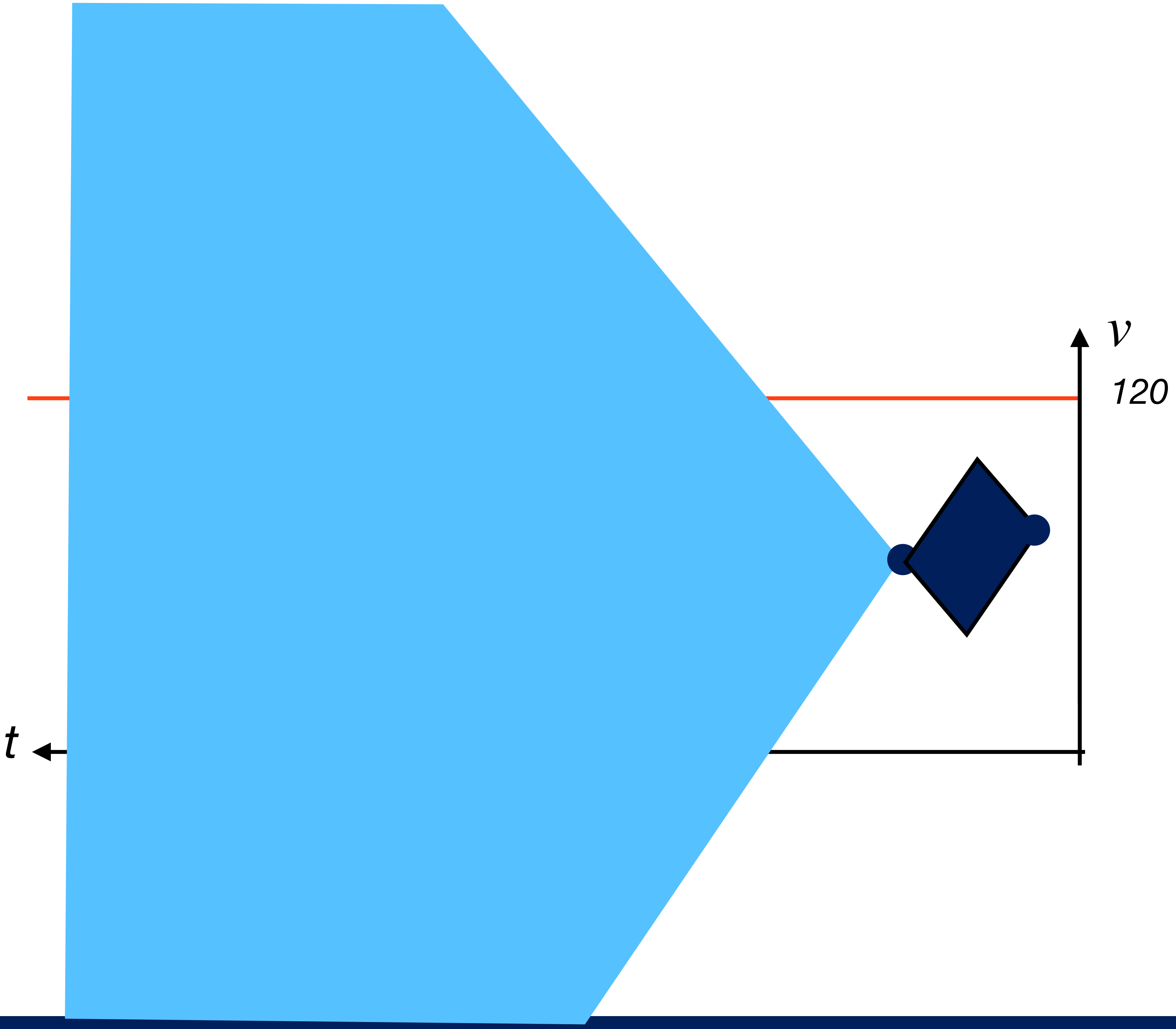
Algorithm: Bounded-time Reachability



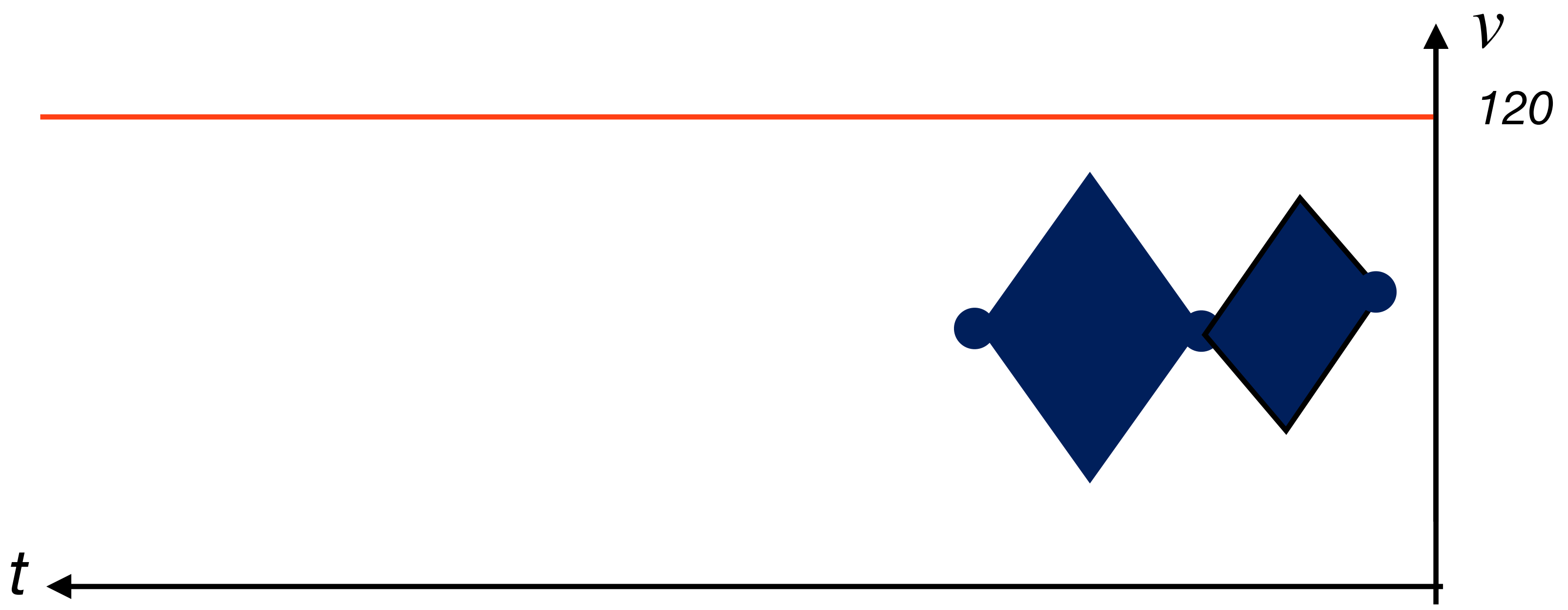
Algorithm: Bounded-time Reachability



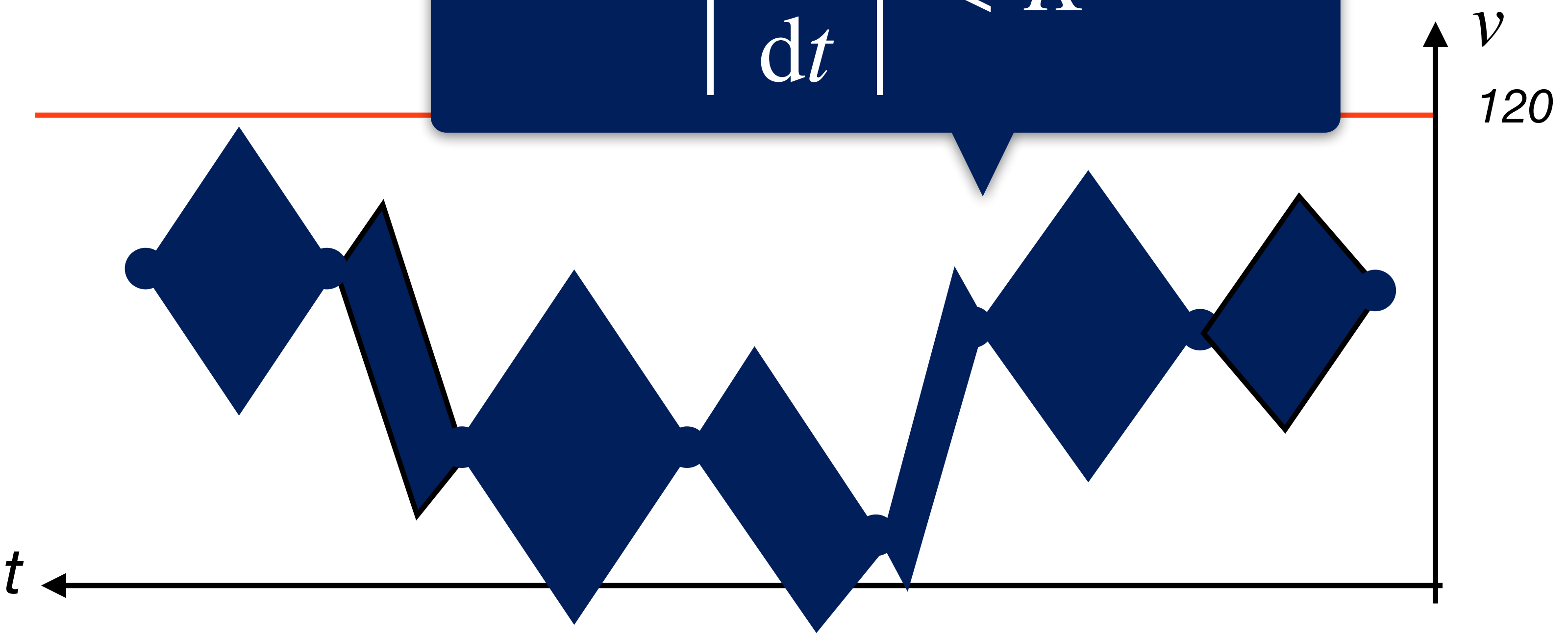
Algorithm: Bounded-time Reachability



Algorithm: Bounded-time Reachability



Algorithm: Bounded-time Reachability



Feasible execution with
$$\left|\frac{\mathrm{d}v}{\mathrm{d}t}\right| < K$$

Implementations

Approach 1: Utilize existing model-checker (PHAVerLite)

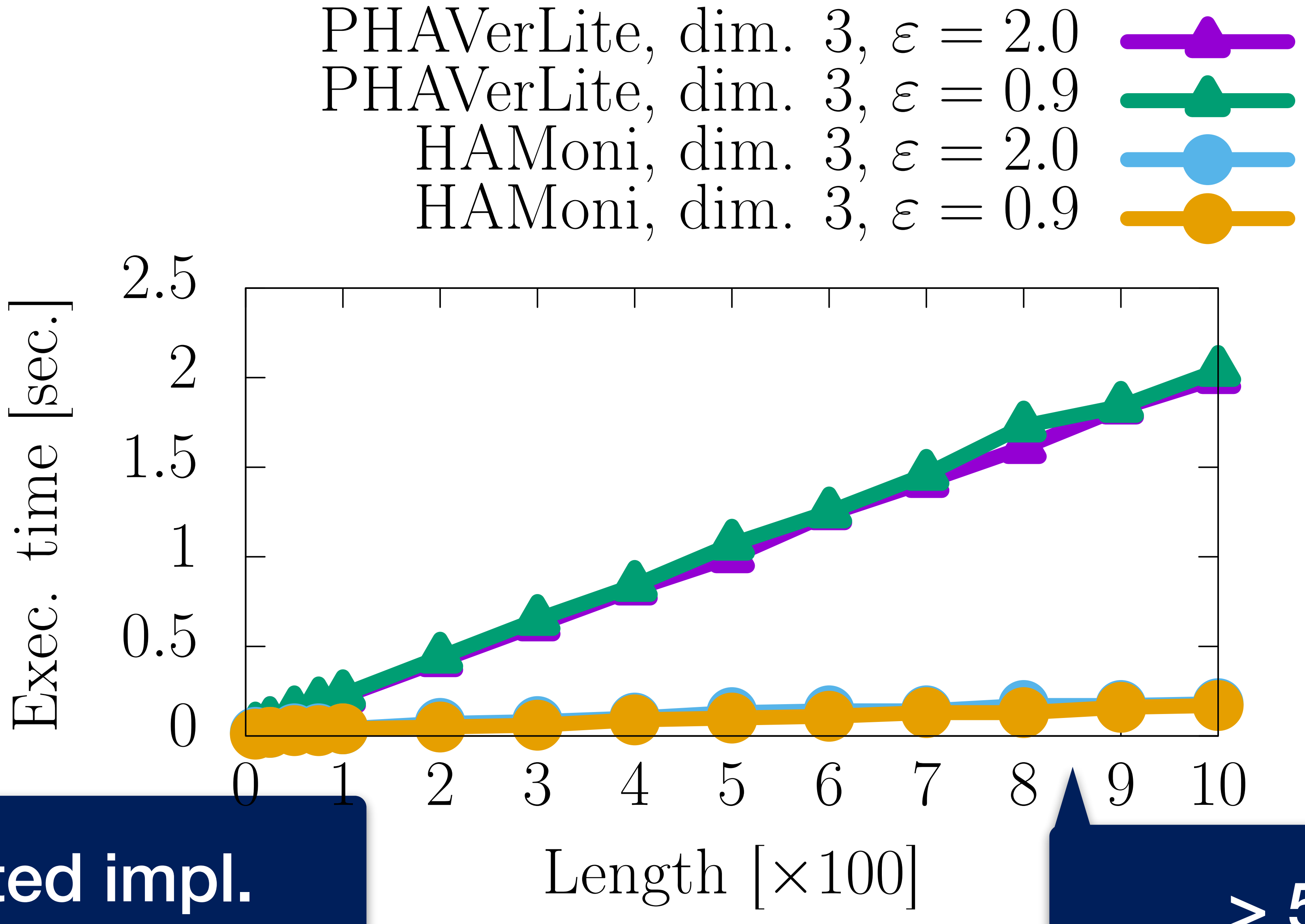
Pros: Highly-optimized reachability analysis impl.

Approach 2: Implement dedicated monitor (HAMoni)

Pros: Best performance in theory

Experiment Results

Changing Observation Length

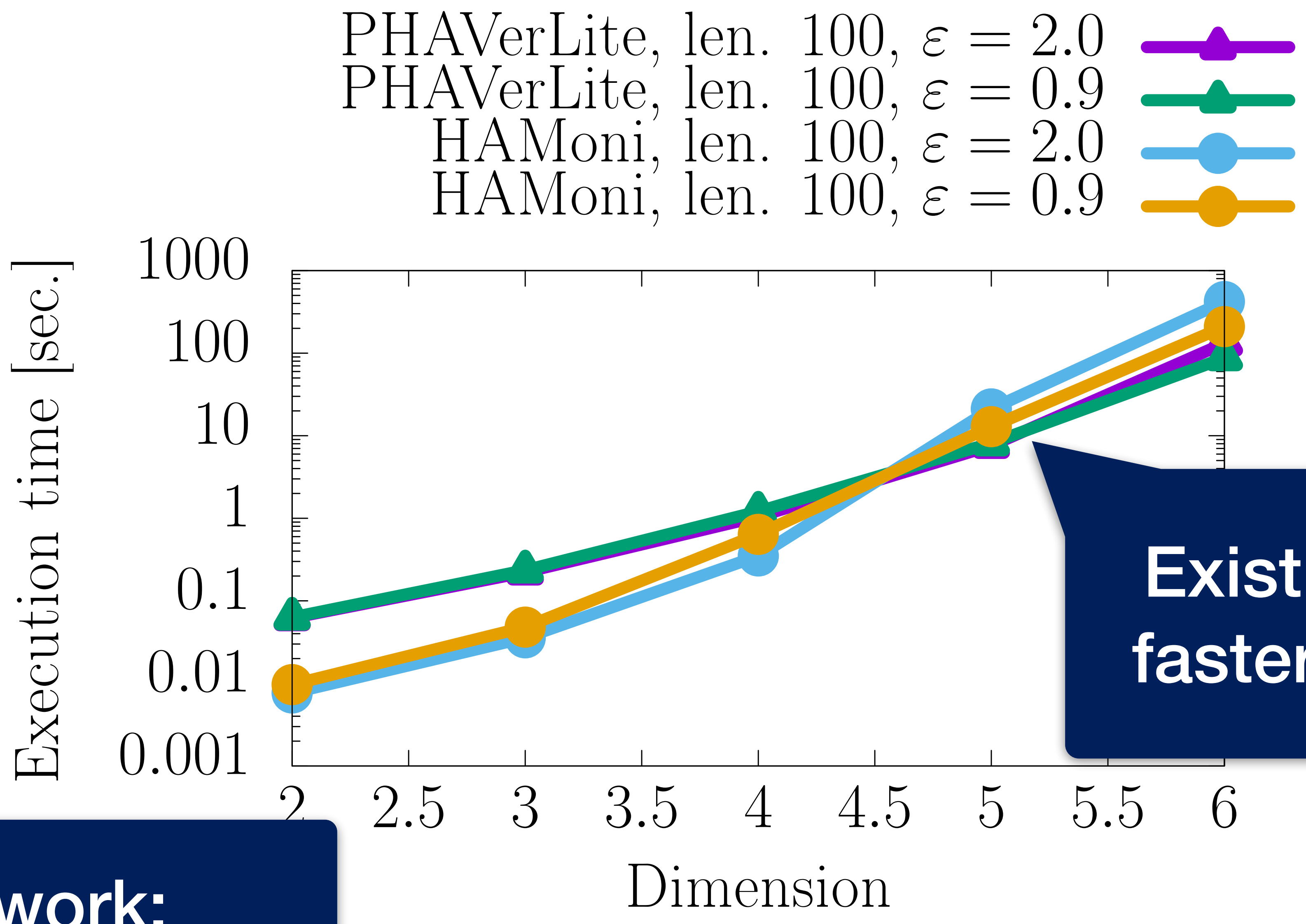


Dedicated impl.
≈ 10x faster

> 5000
samples / sec.

Experiment Results

Changing Model Dimension



Existing tool was faster for dim. > 6

Future work: further optimization

Conclusions

- Proposed model-bounded monitoring

  Bounding model (knowledge): linear HAs $\mathscr{M}$

- Algorithms + implementations

  Idea: bounded-time reachability

- Experiment → effectively monitorable