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]

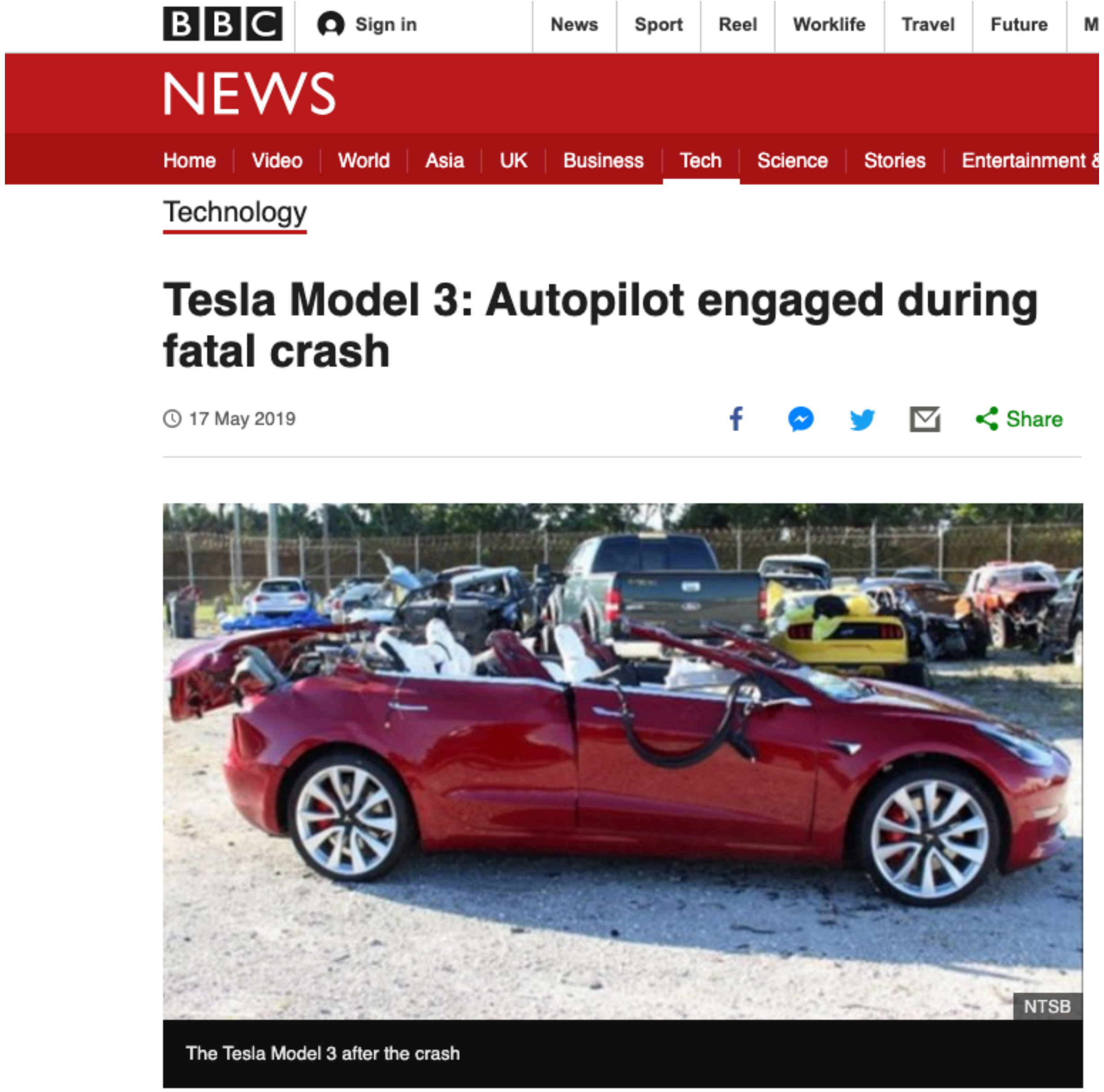
18 May 2021, MT-CPS 2021

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

Photo by: Air15



Technology

Tesla Model 3: Autopilot engaged during fatal crash

17 May 2019

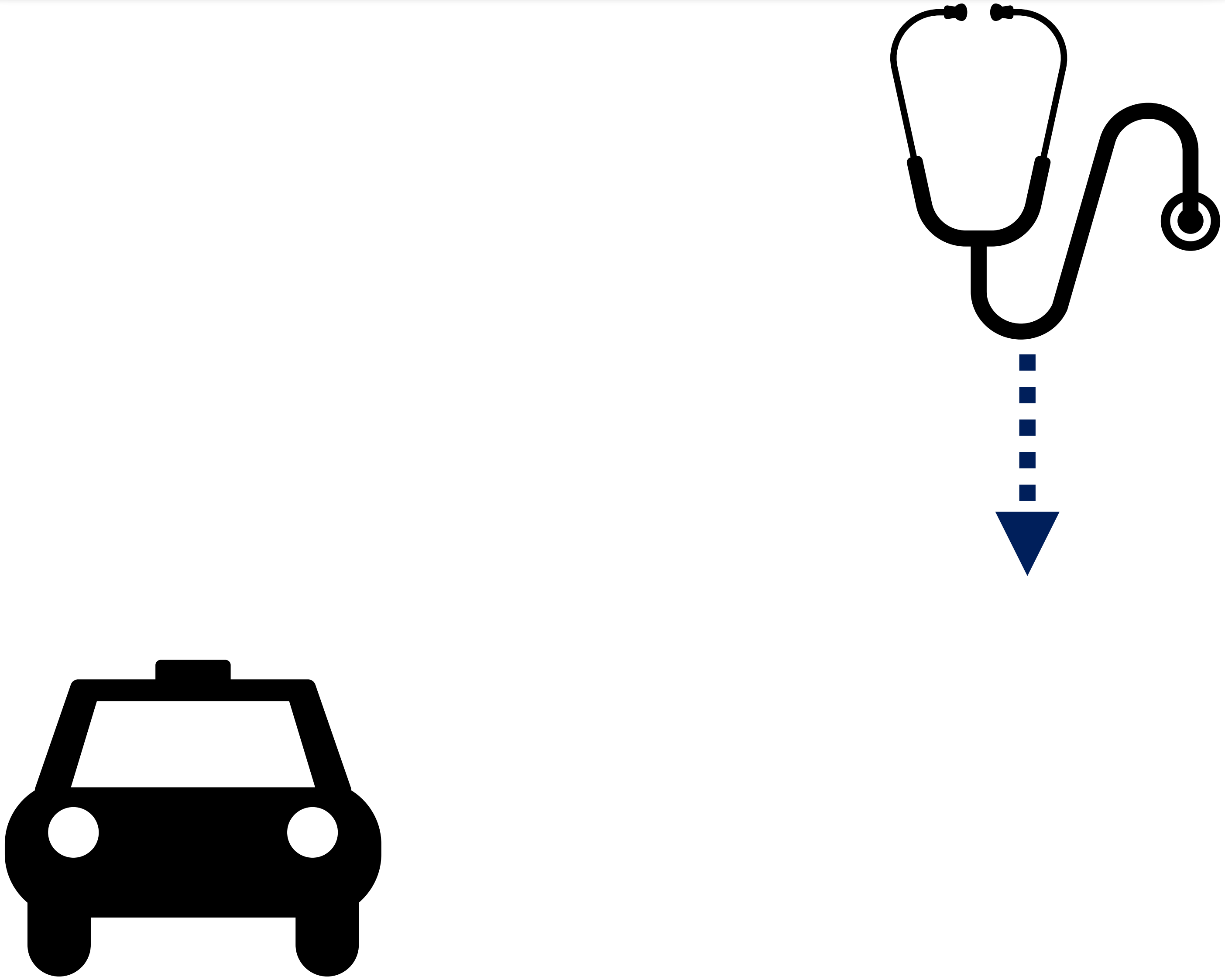
The Tesla Model 3 after the crash

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

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

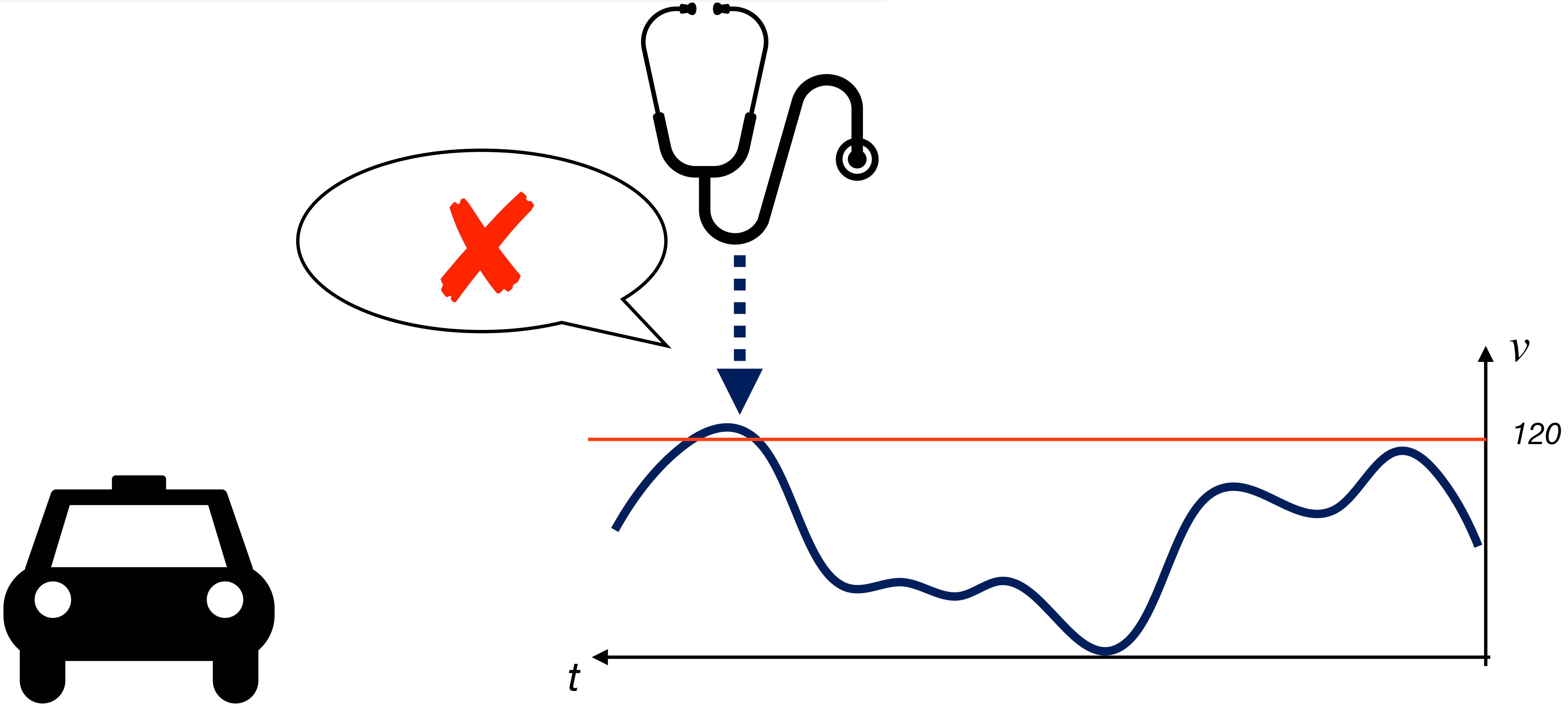
Monitoring

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



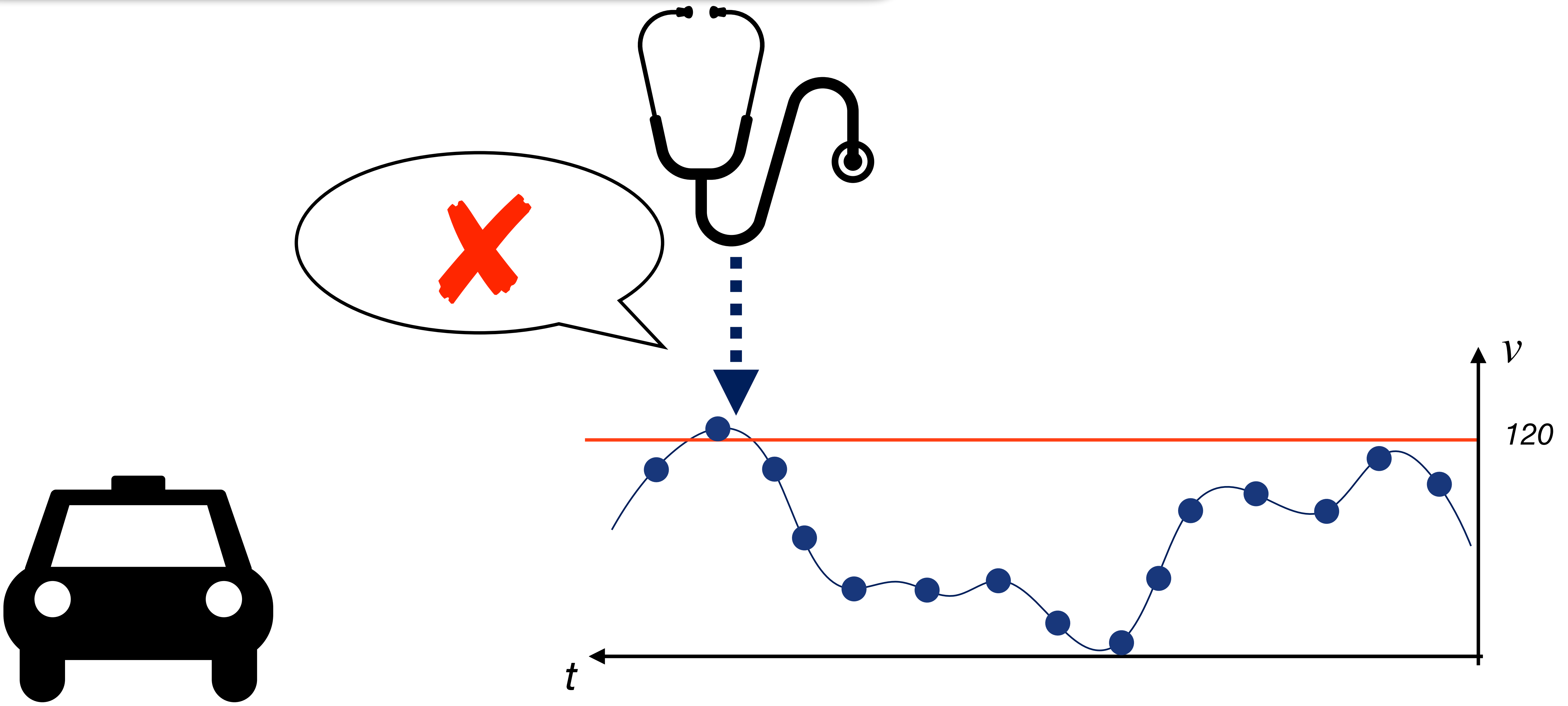
Monitoring

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



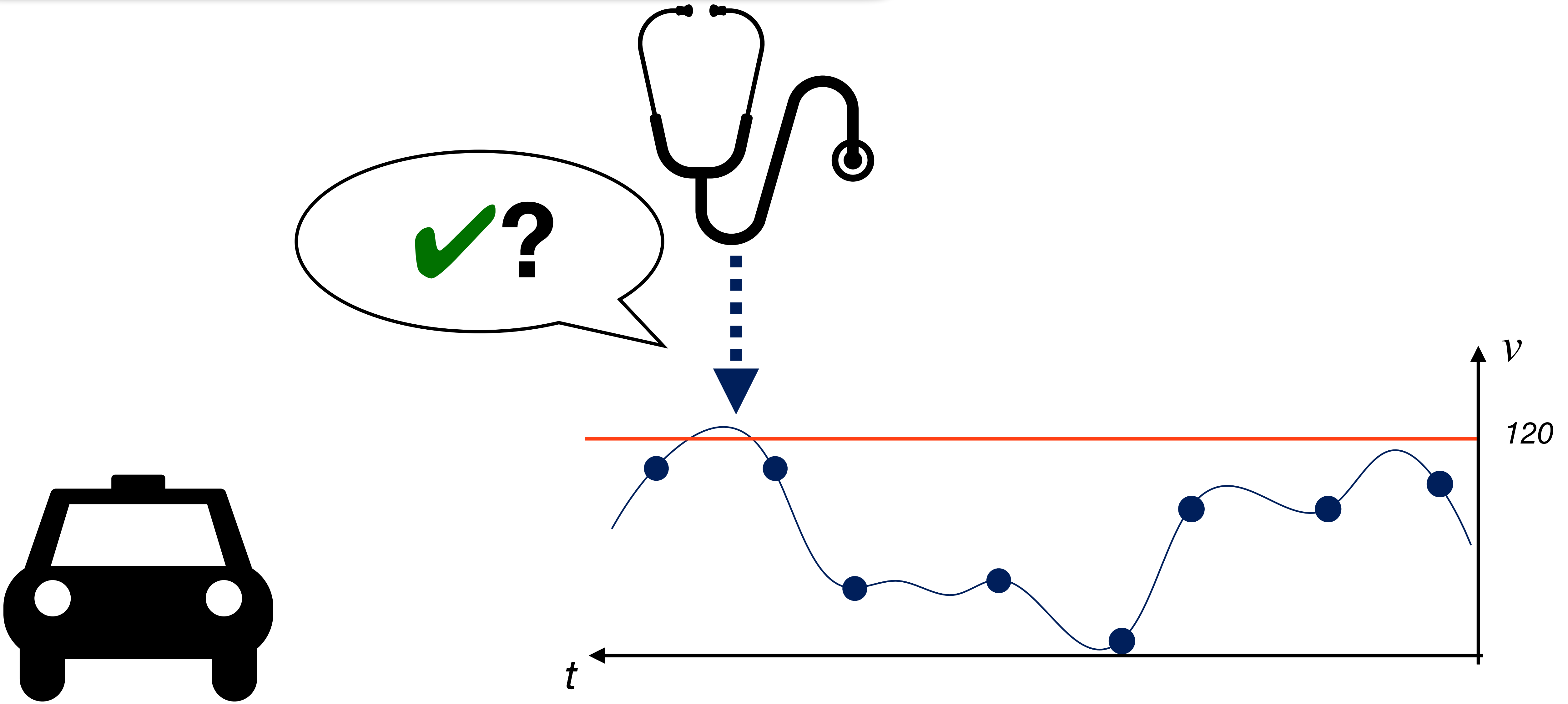
Monitoring with Sampling

Specification: No $(v > 120)$



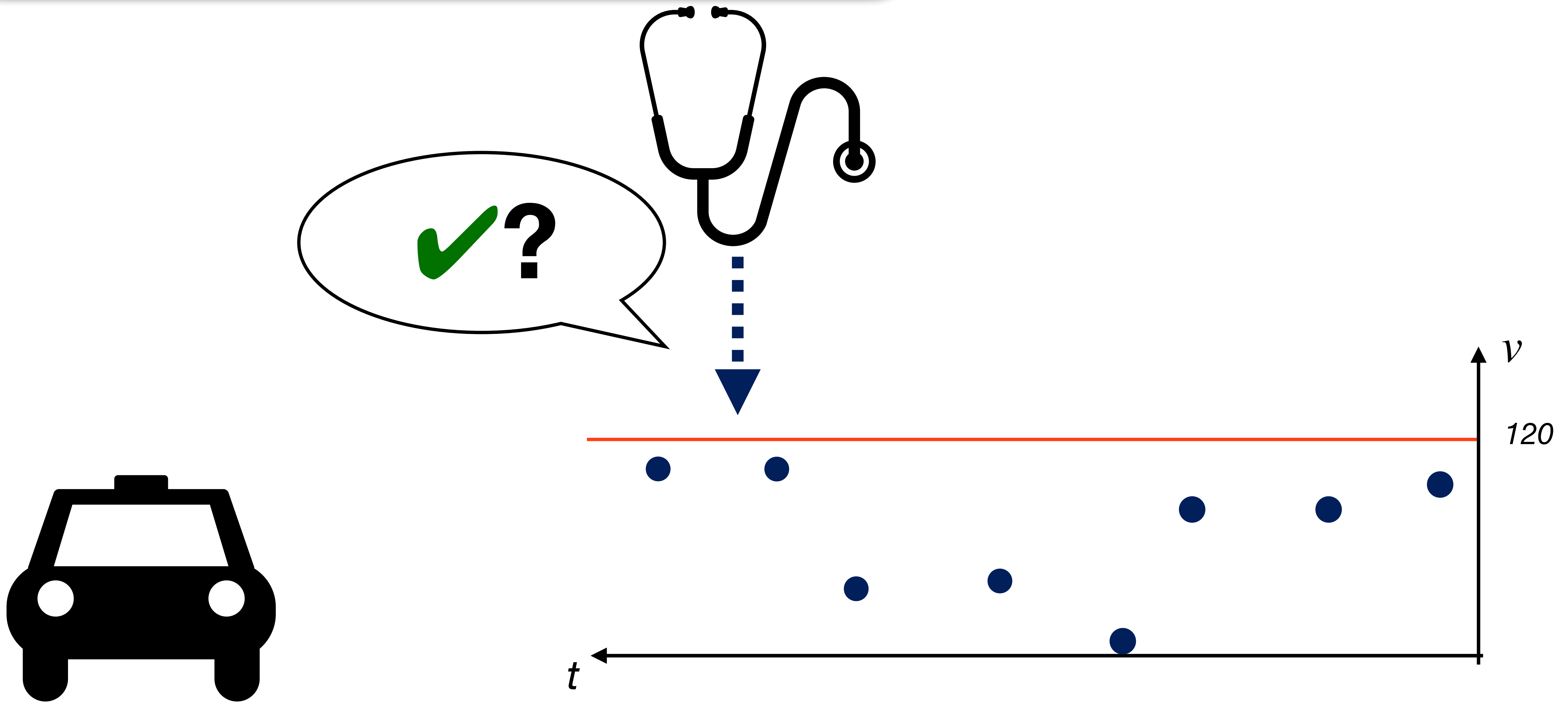
Monitoring with Sampling

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



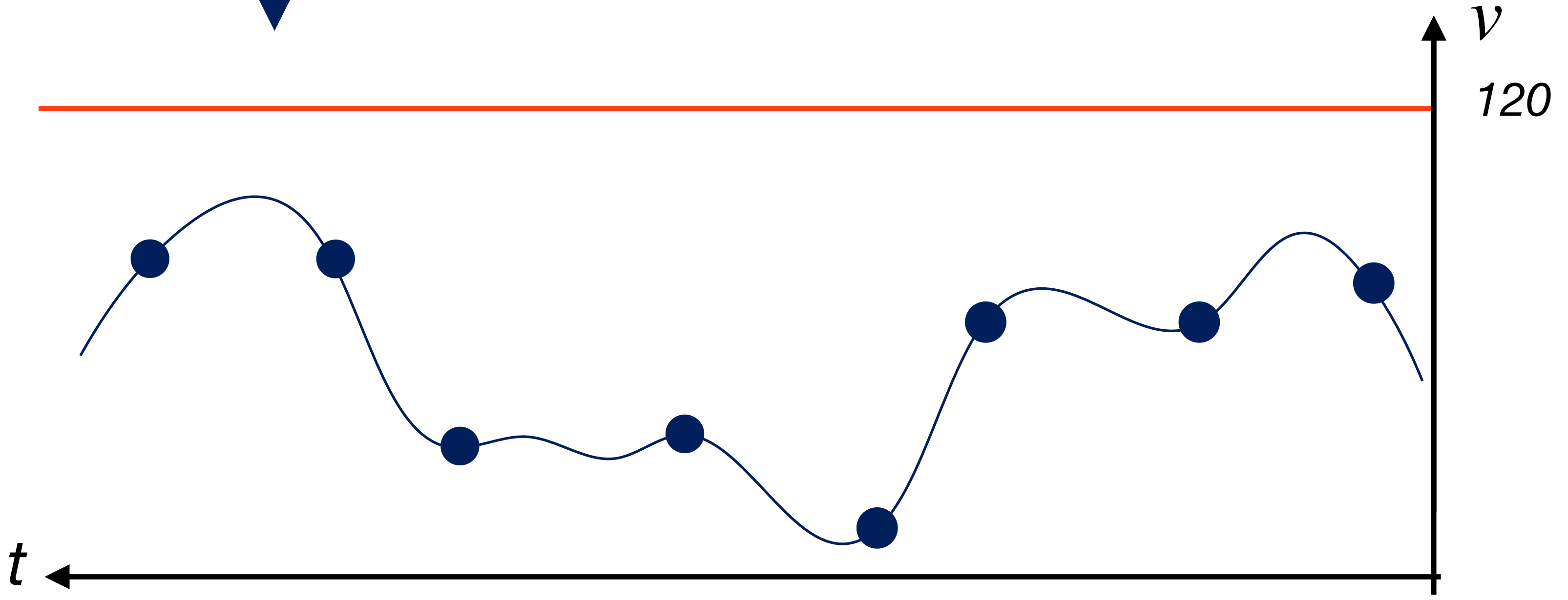
Monitoring with Sampling

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



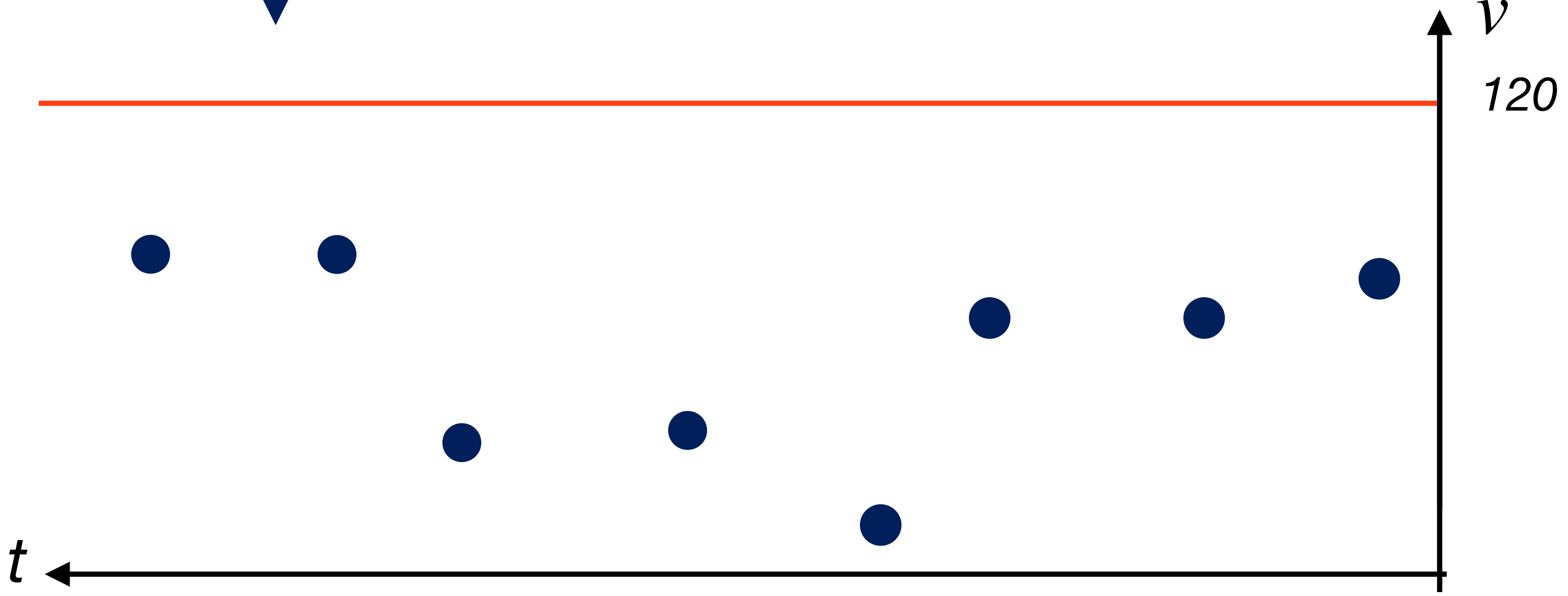
Signal Interpolation

Specification: No $(v > 120)$



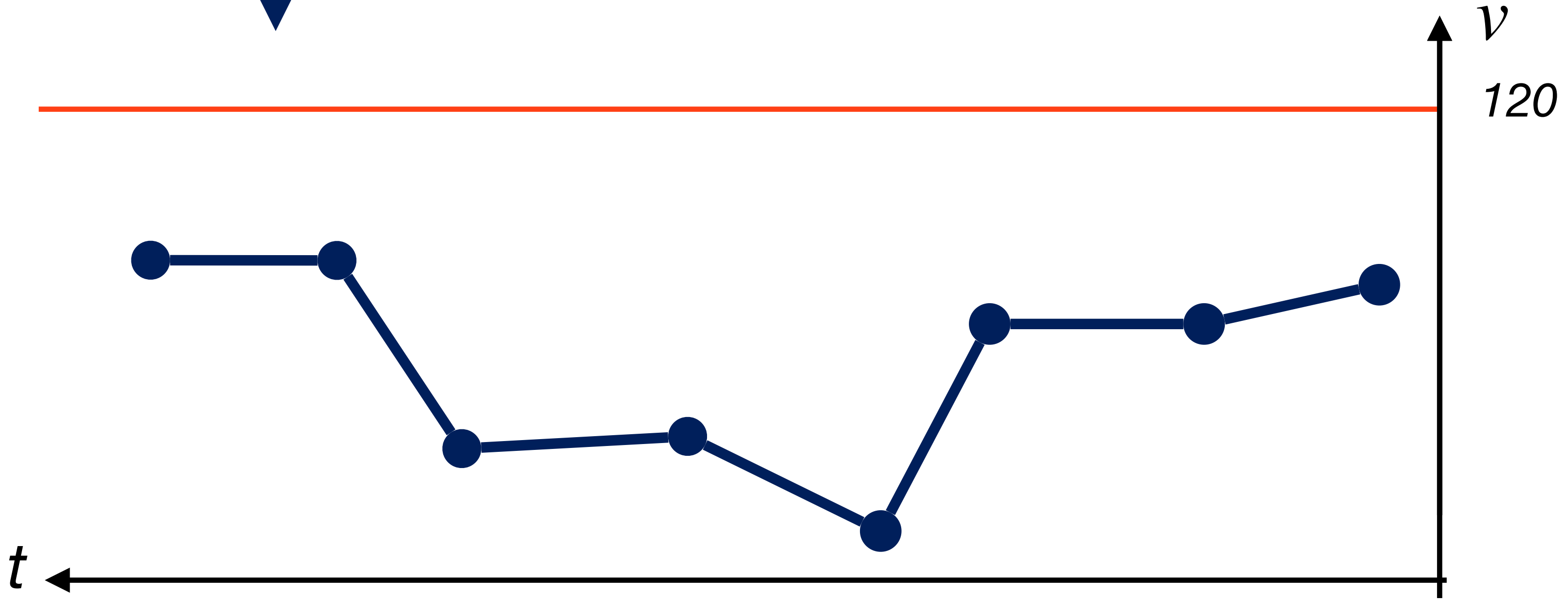
Signal Interpolation

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



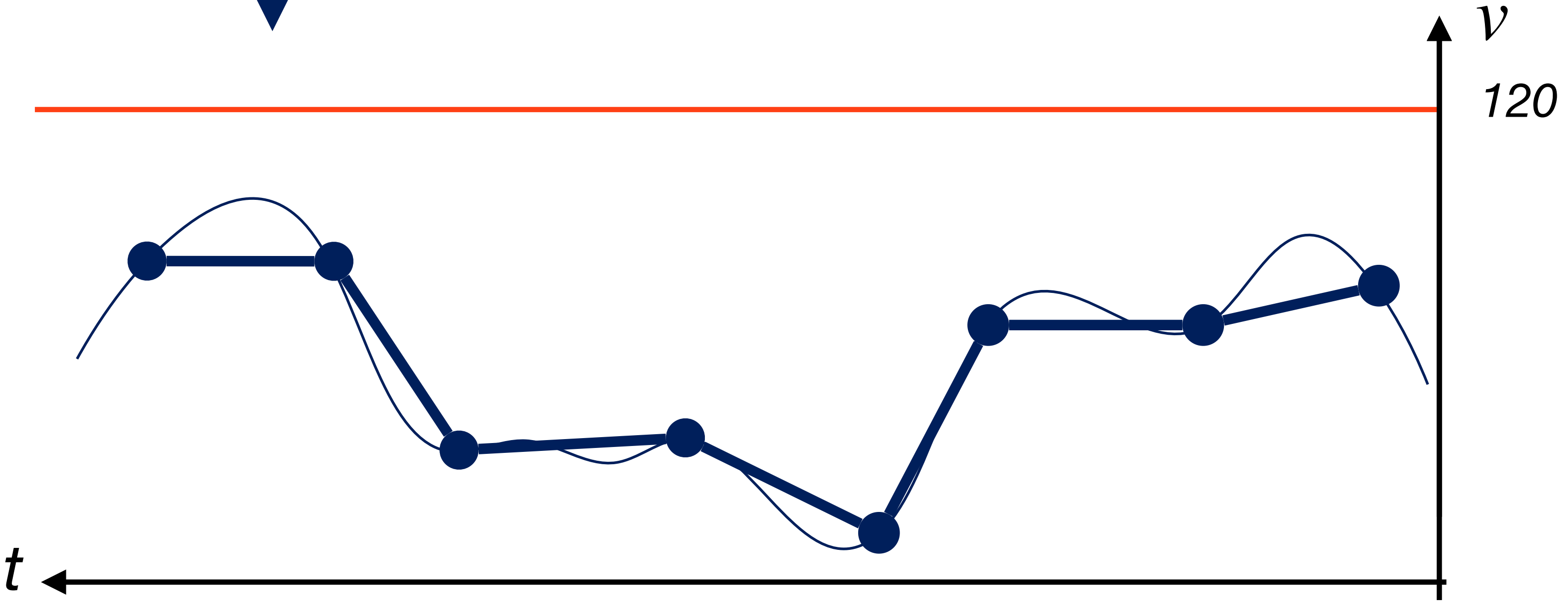
Signal Interpolation

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



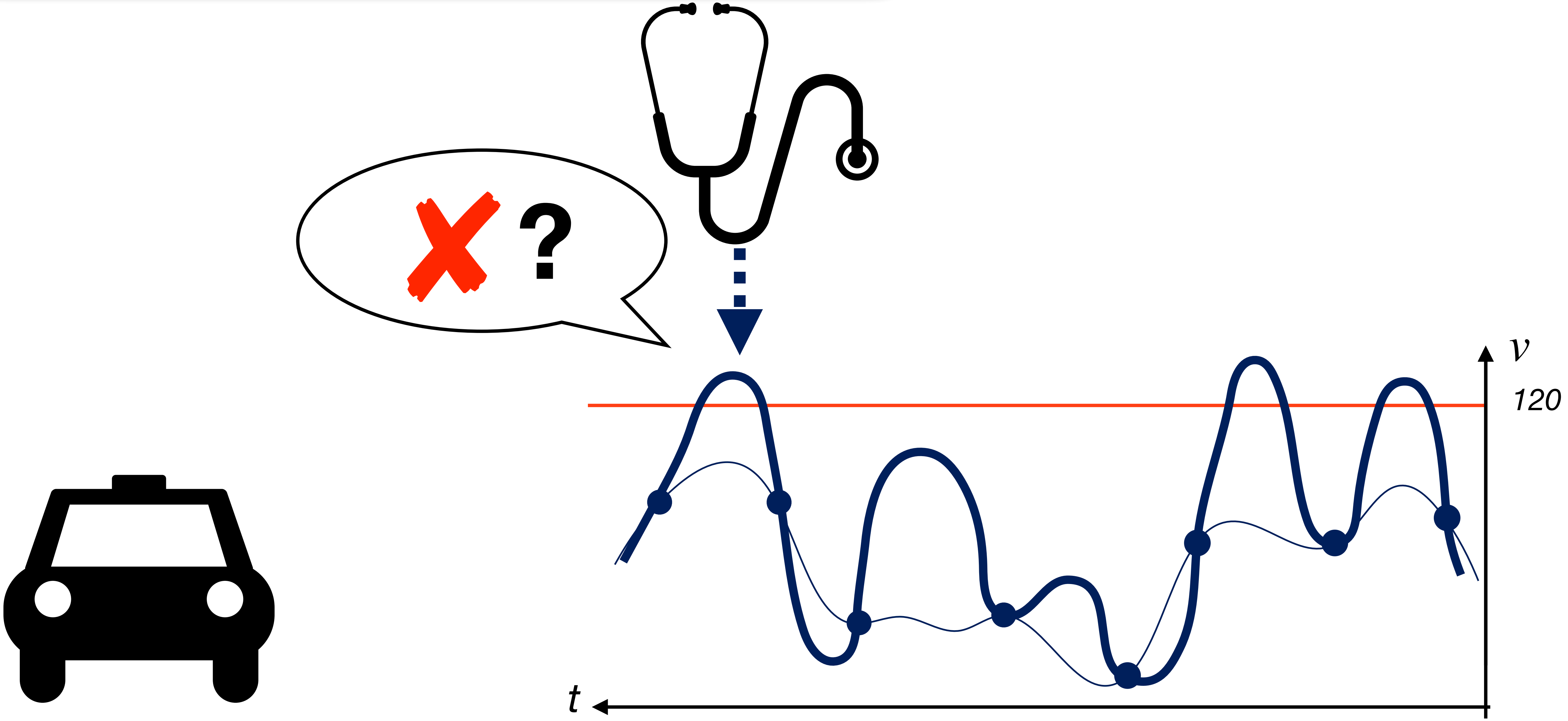
Signal Interpolation

Specification: No $(v > 120)$



Signal Interpolation

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

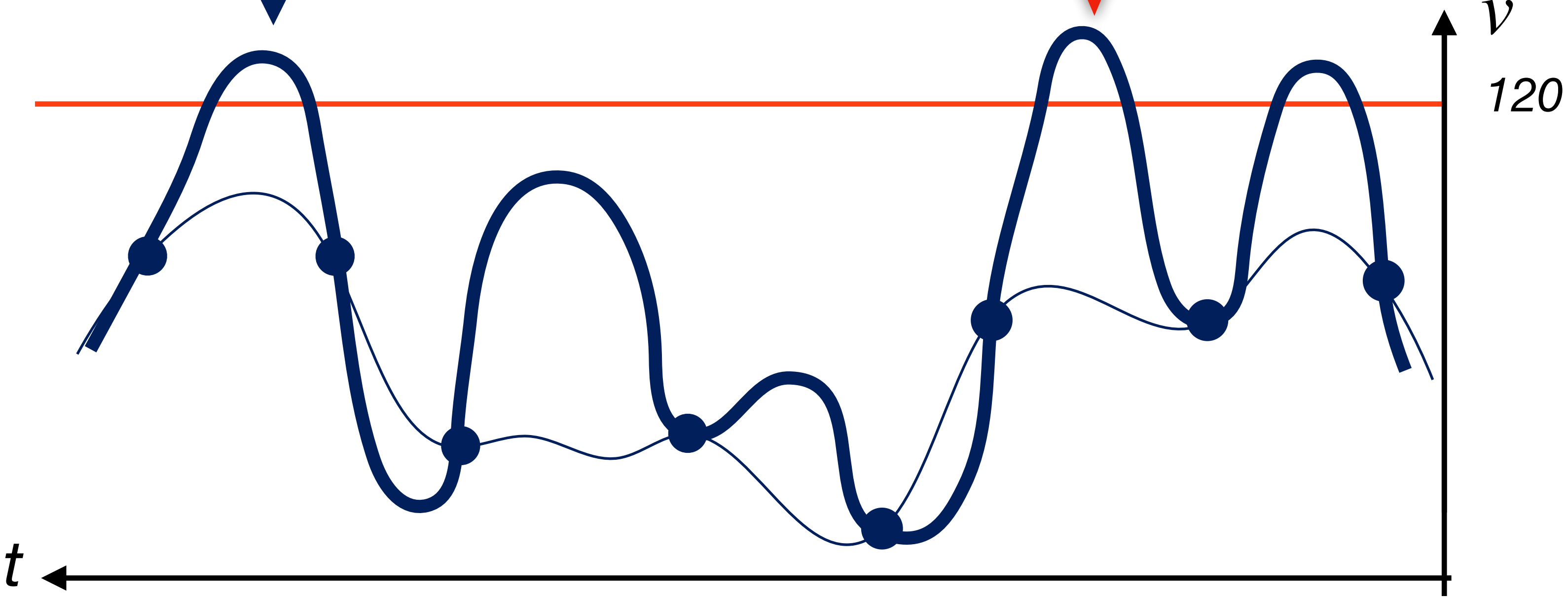


Interpolation with Prior Knowledge

Specification: No $(v > 120)$

Impossible because

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



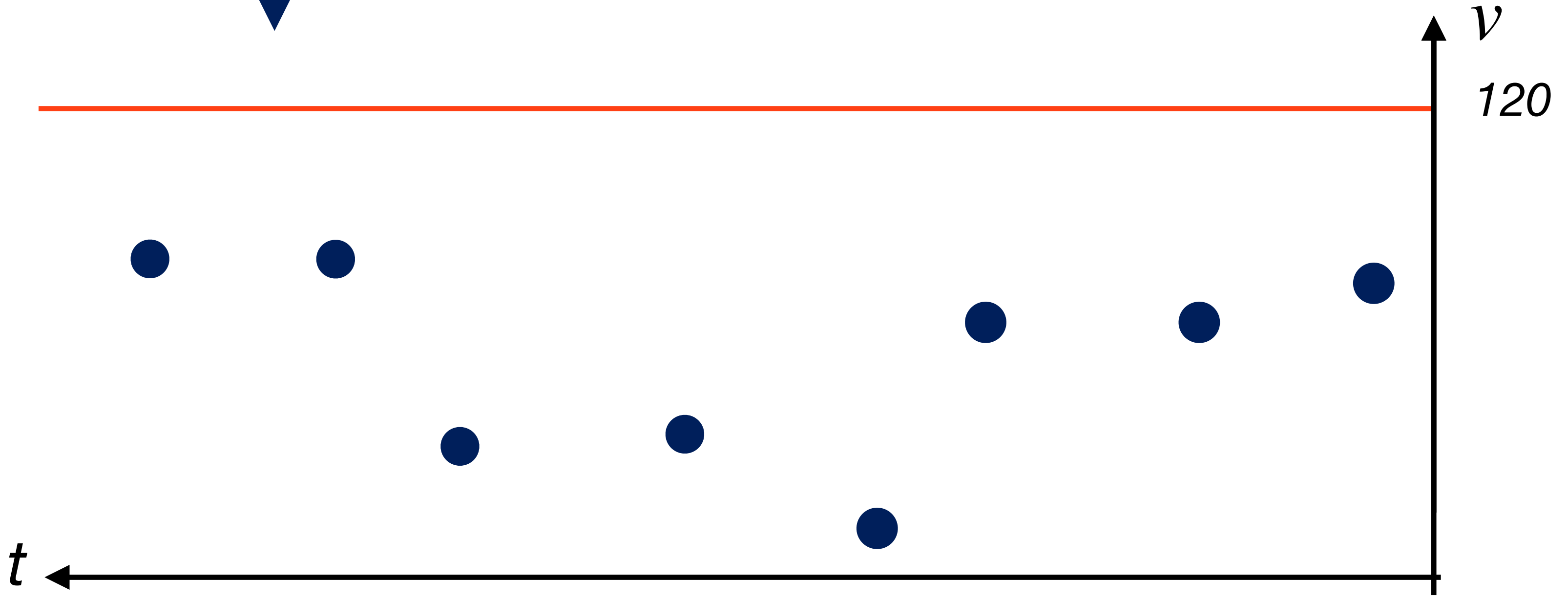
Model-Bounded Monitoring

Our Contribution

Specification: No $(v > 120)$

Knowledge (bounding model)

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



Model-Bounded Monitoring

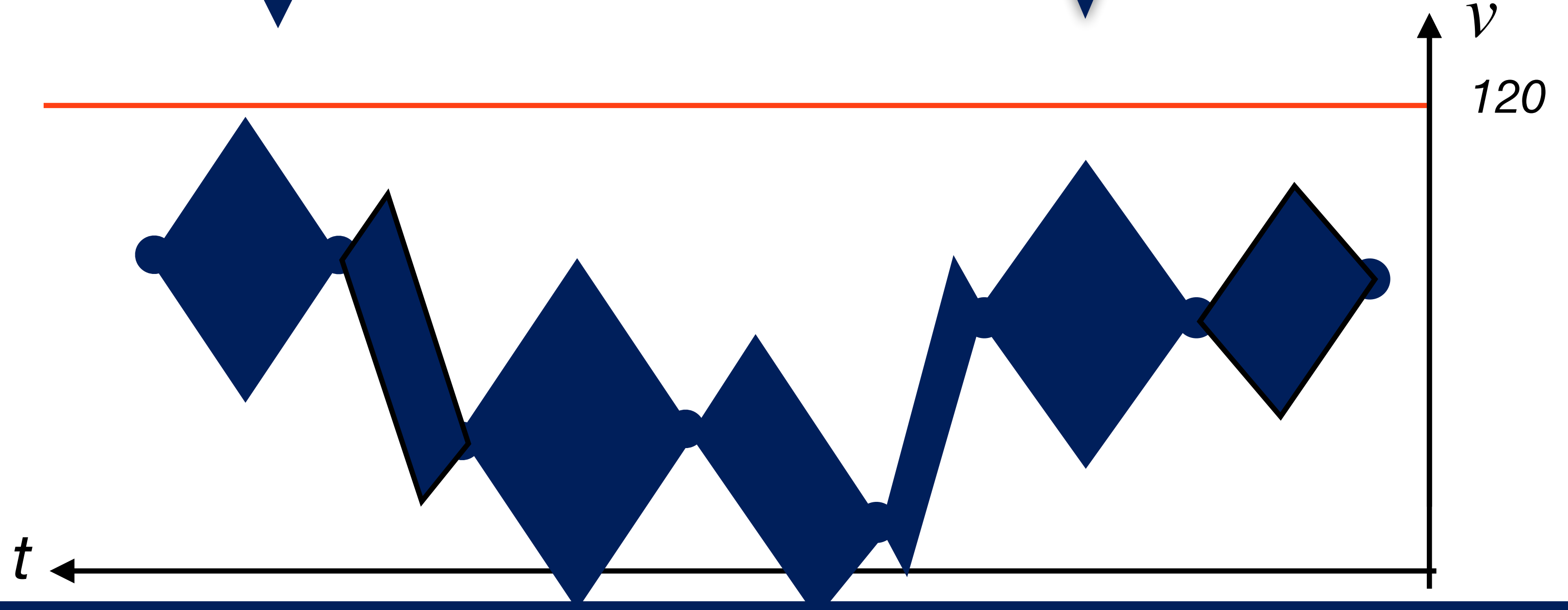
Our Contribution

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

Specification: No $(v > 120)$

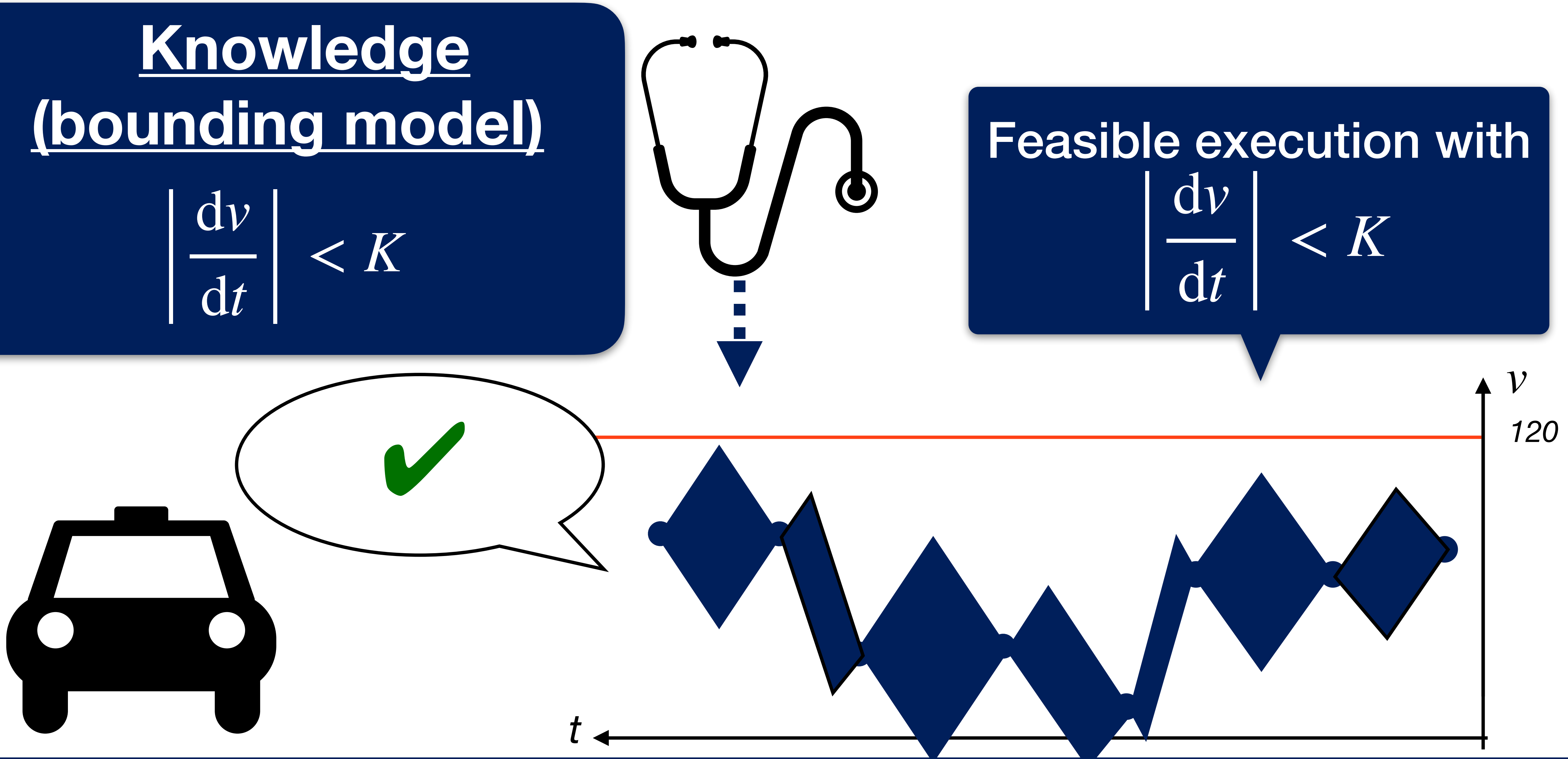
Our Contribution

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?

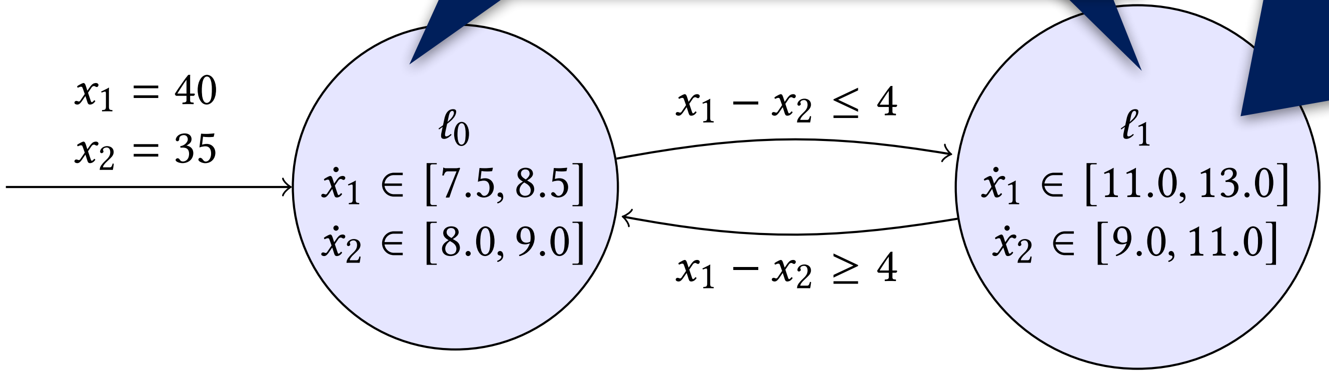
Knowledge (bounding model)

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

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
$\dot{x}_1 \in [11.0, 13.0]$
$\dot{x}_2 \in [9.0, 11.0]$

Contributions

- Proposed model-bounded monitoring

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

- Formalized with monitored language $L_{\mathrm{mon}}(\mathscr{M})$

  $L_{\mathrm{mon}}(\mathscr{M})$: possible *discrete* observations of $\mathscr{M}$

- Algorithms + implementations

  Idea: bounded-time reachability
  Experiment → effectively monitorable

Model-Bounded Monitoring

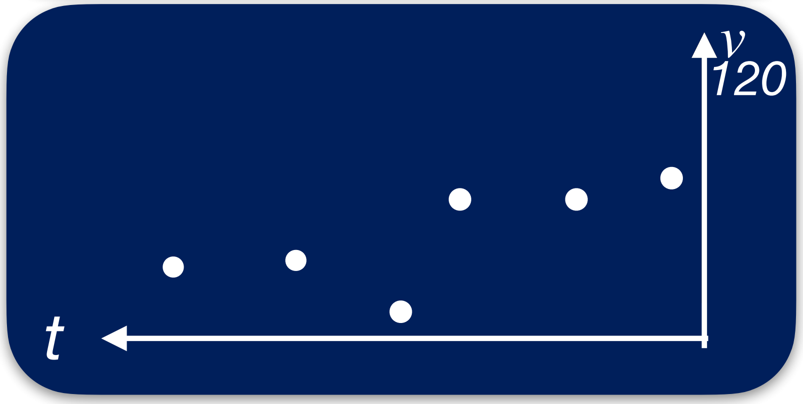
Our Contribution

Given

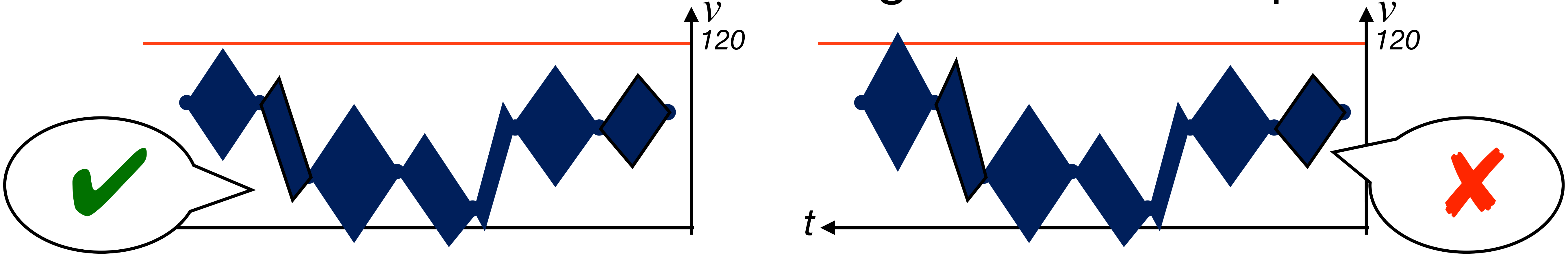
- Bounding model in LHA $\mathscr{M}$
- Safety Specification φ
- Discrete Log w

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

No $(v > 120)$



Decide if the actual behavior might violate the spec.



Model-Bounded Monitoring

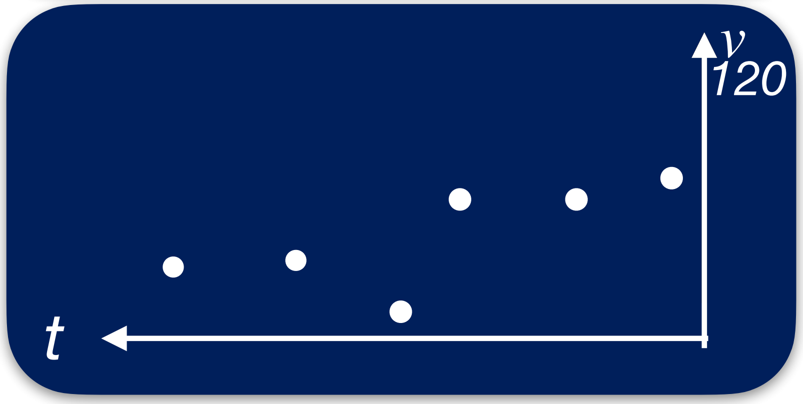
Given

- Bounding model in LHA $\mathscr{M}$
- Safety Specification φ
- Discrete Log w

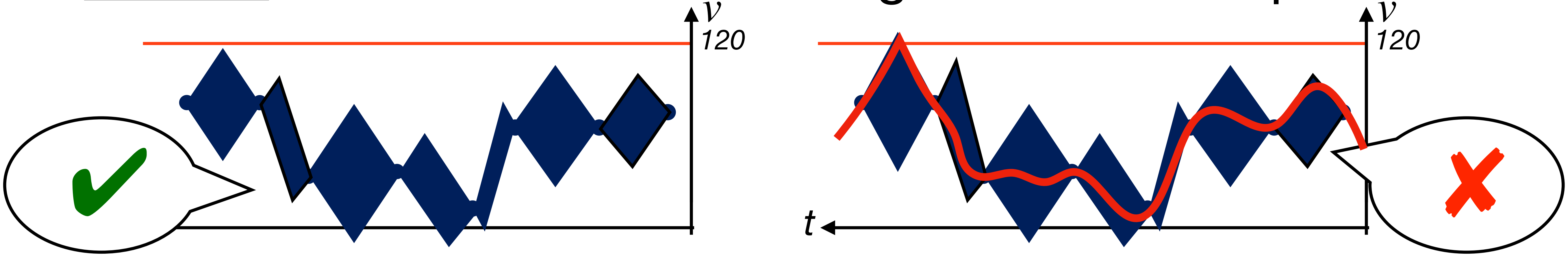
Our Contribution

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

No $(v > 120)$



Decide if the actual behavior might violate the spec.



Monitored Language L_{mon}

Our Contribution

Combine cont. exec. of $\mathscr{M}$ and disc. obs. of w

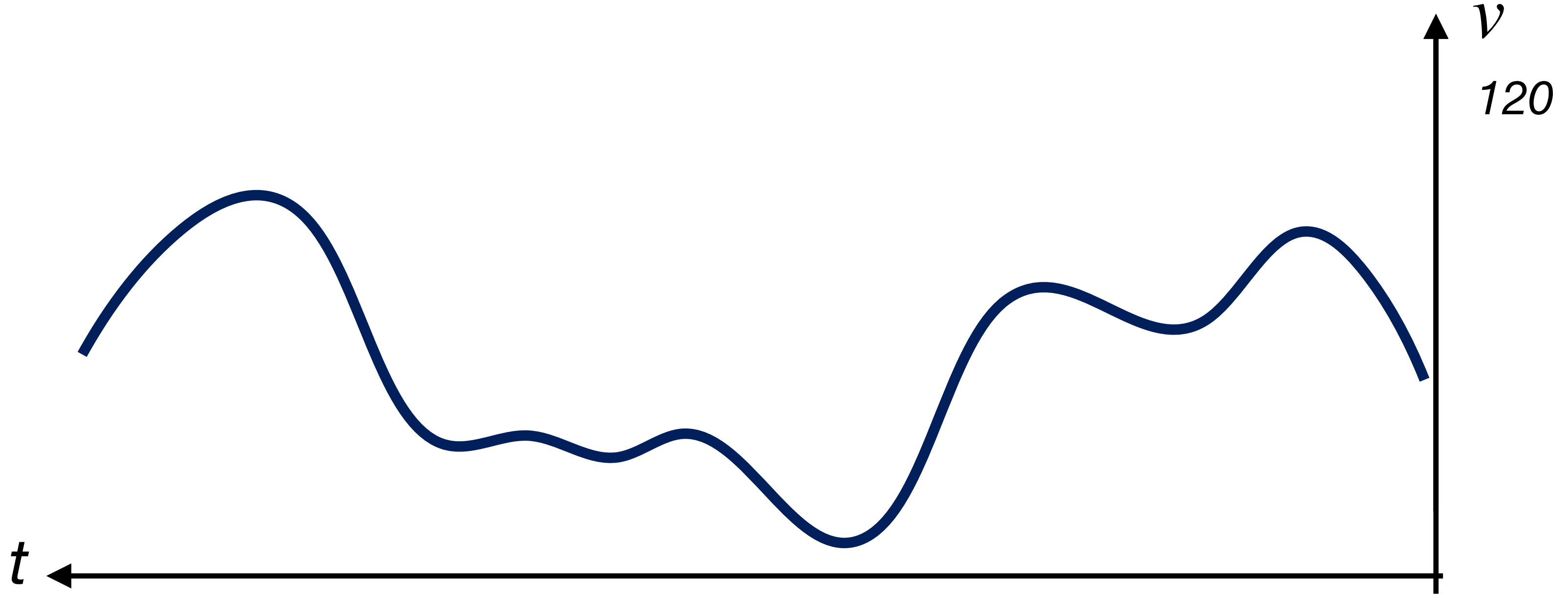
$L_{\mathrm{mon}}(\mathscr{M}) = \{$ Discr. Obs w |

Monitored Language L_{mon}

Our Contribution

Combine cont. exec. of $\mathscr{M}$ and disc. obs. of w

$L_{\mathrm{mon}}(\mathscr{M}) =$ { Discr. Obs w | ∃ exec. σ of $\mathscr{M}$ s.t.

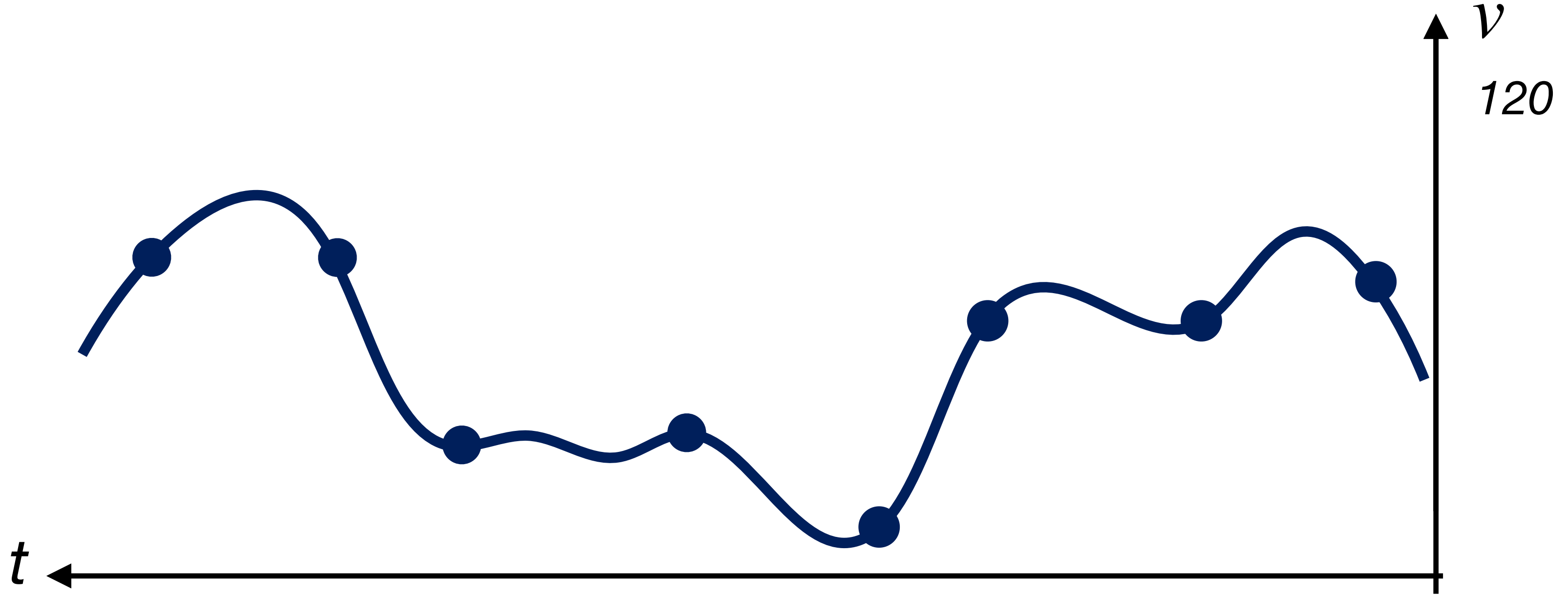


Monitored Language L_{mon}

Our Contribution

Combine cont. exec. of $\mathscr{M}$ and disc. obs. of w

$L_{\mathrm{mon}}(\mathscr{M}) = \{$ Discr. Obs $w \mid \exists$ exec. σ of $\mathscr{M}$ s.t.
w is a sample of $\sigma\ \}$



Workflow of Model-bounded Monitoring

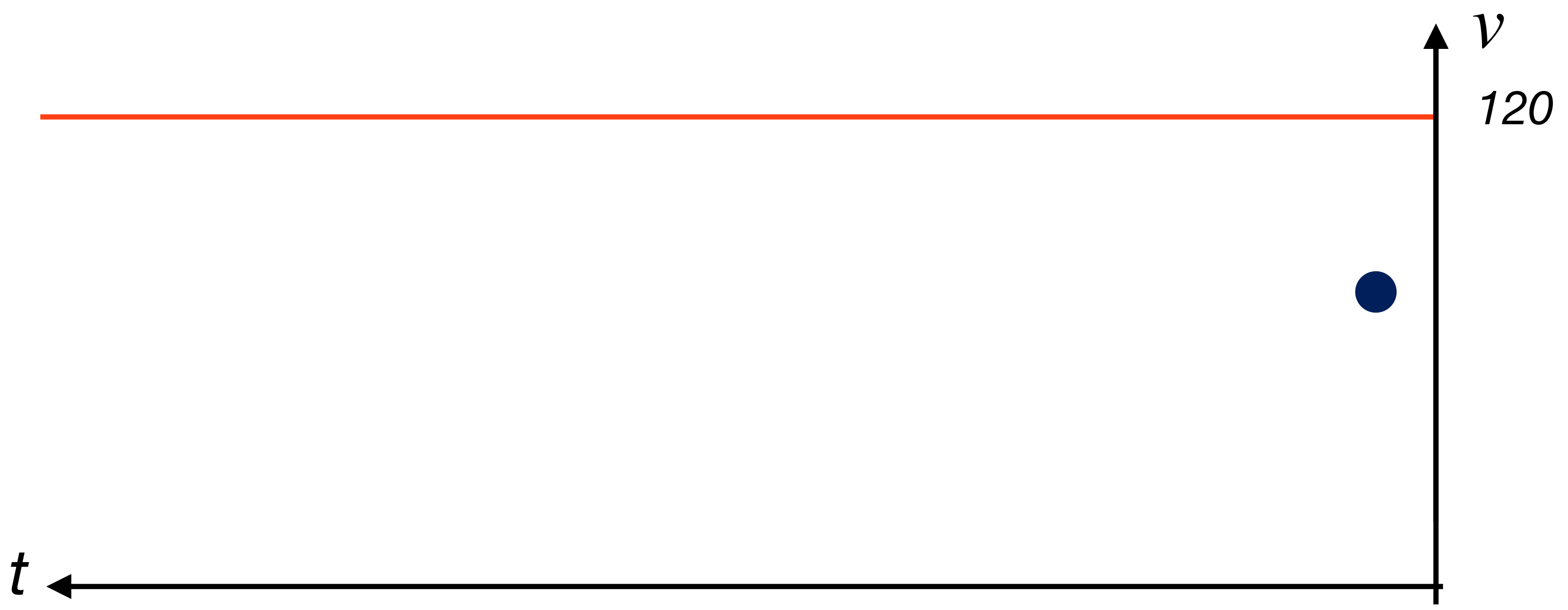
1. Construct an LHA $\mathscr{M}_{\neg\varphi}$ from bounding model $\mathscr{M}$ and spec. φ

   Idea: Product of LHAs

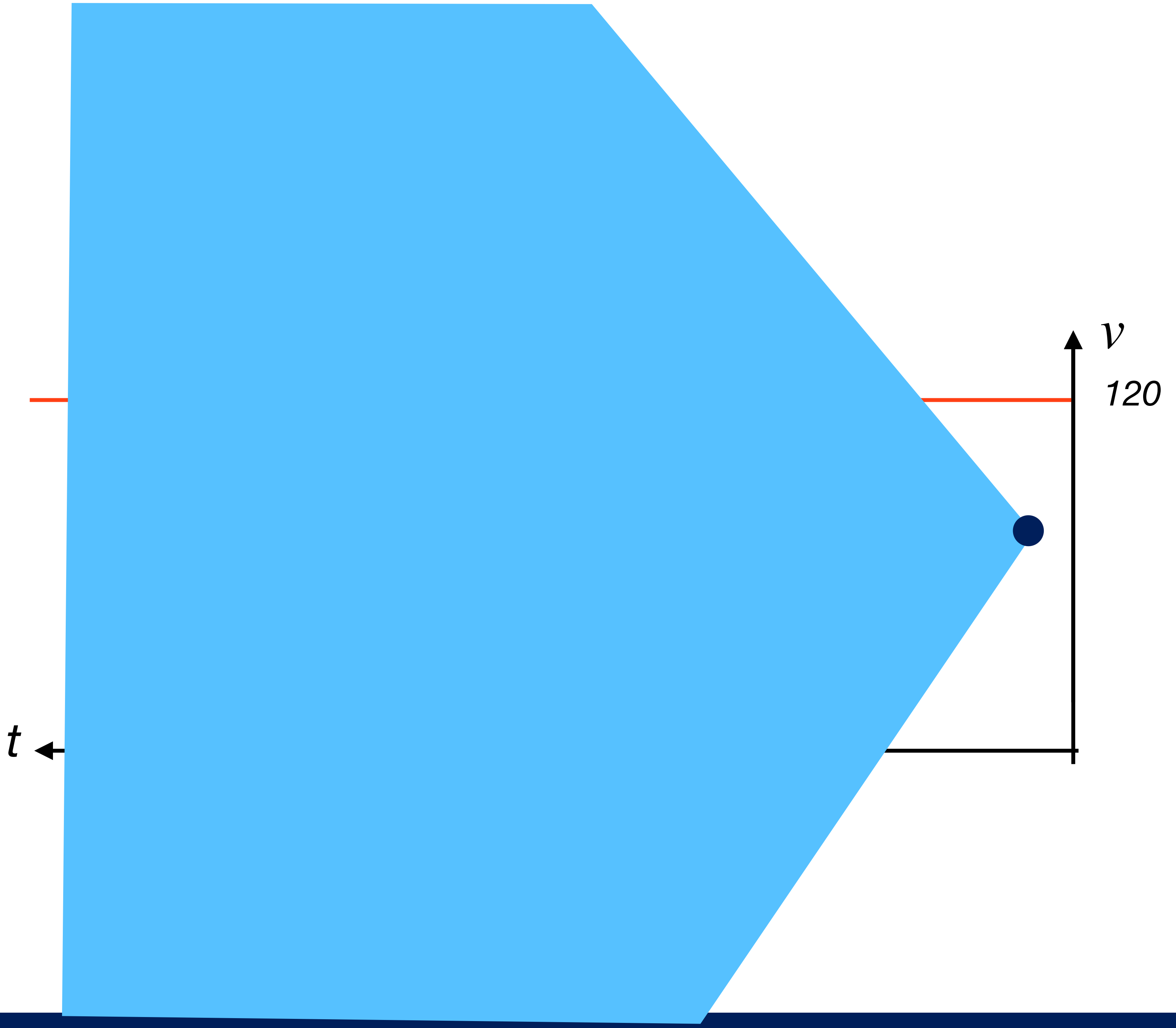
2. Check if $w \in L_{\mathrm{mon}}(\mathscr{M}_{\neg\varphi})$

   Idea: Bounded-time reachability analysis

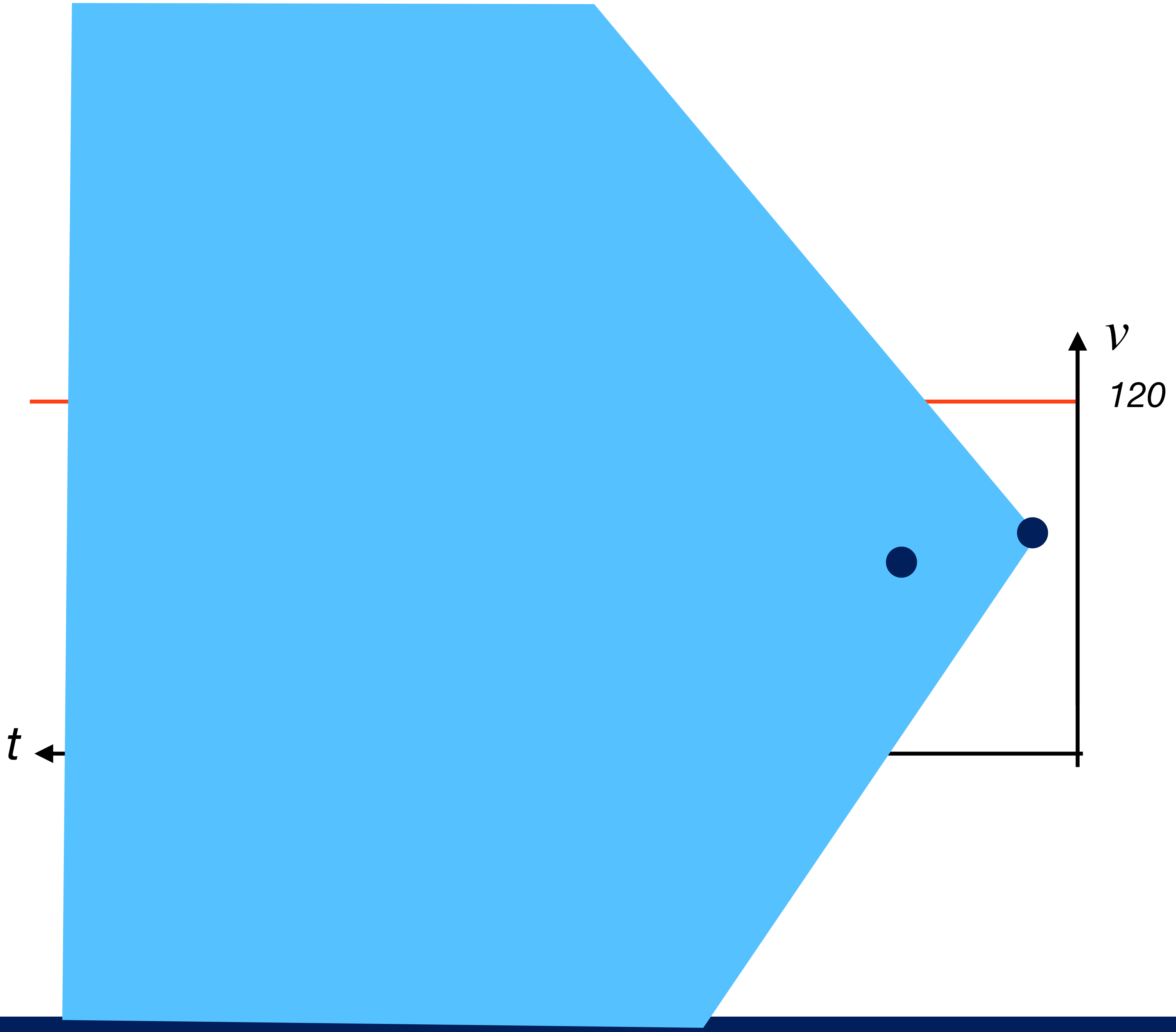
Algorithm: Bounded-time Reachability



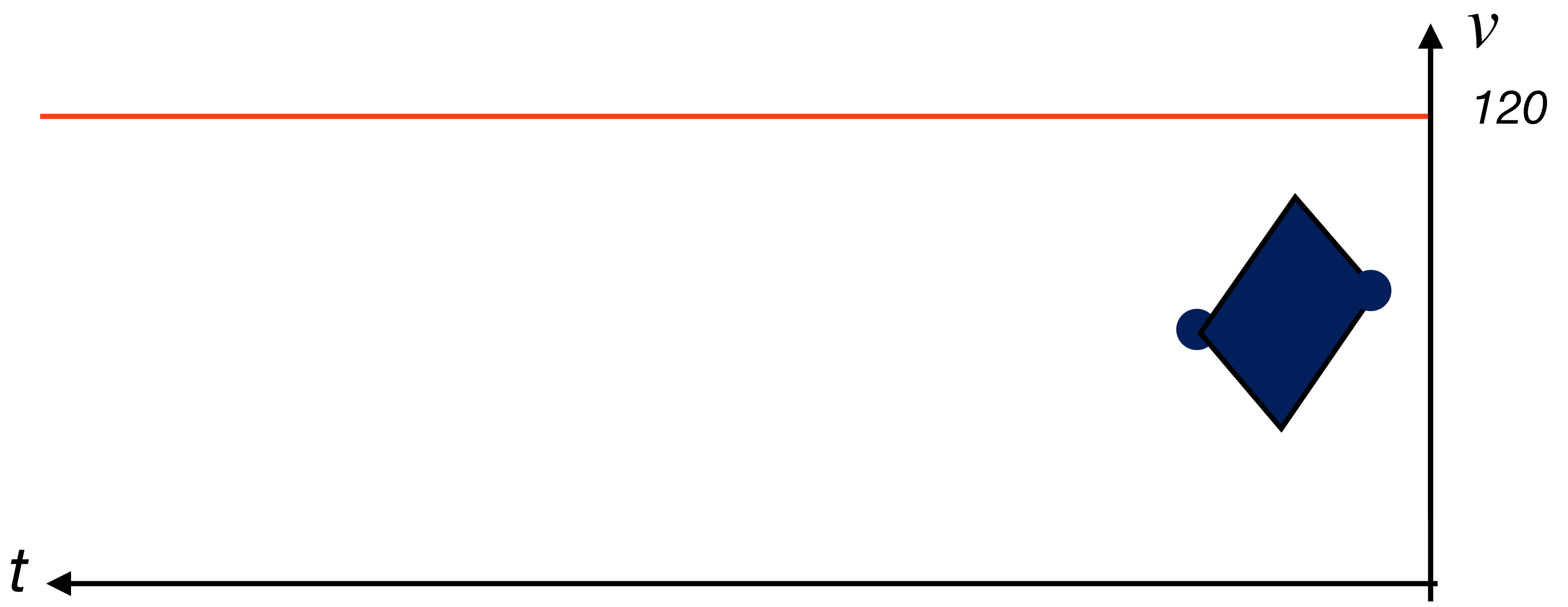
Algorithm: Bounded-time Reachability



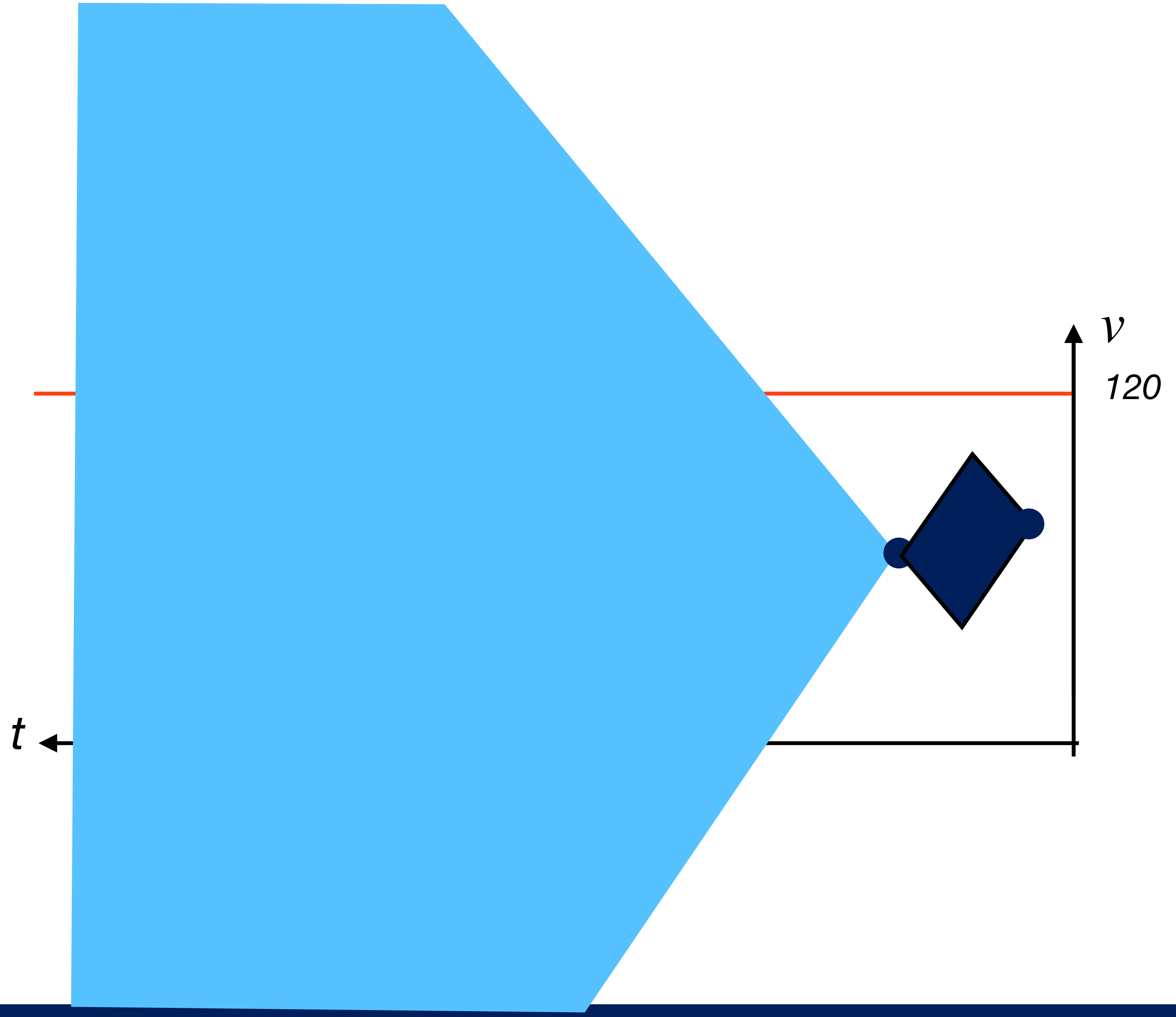
Algorithm: Bounded-time Reachability



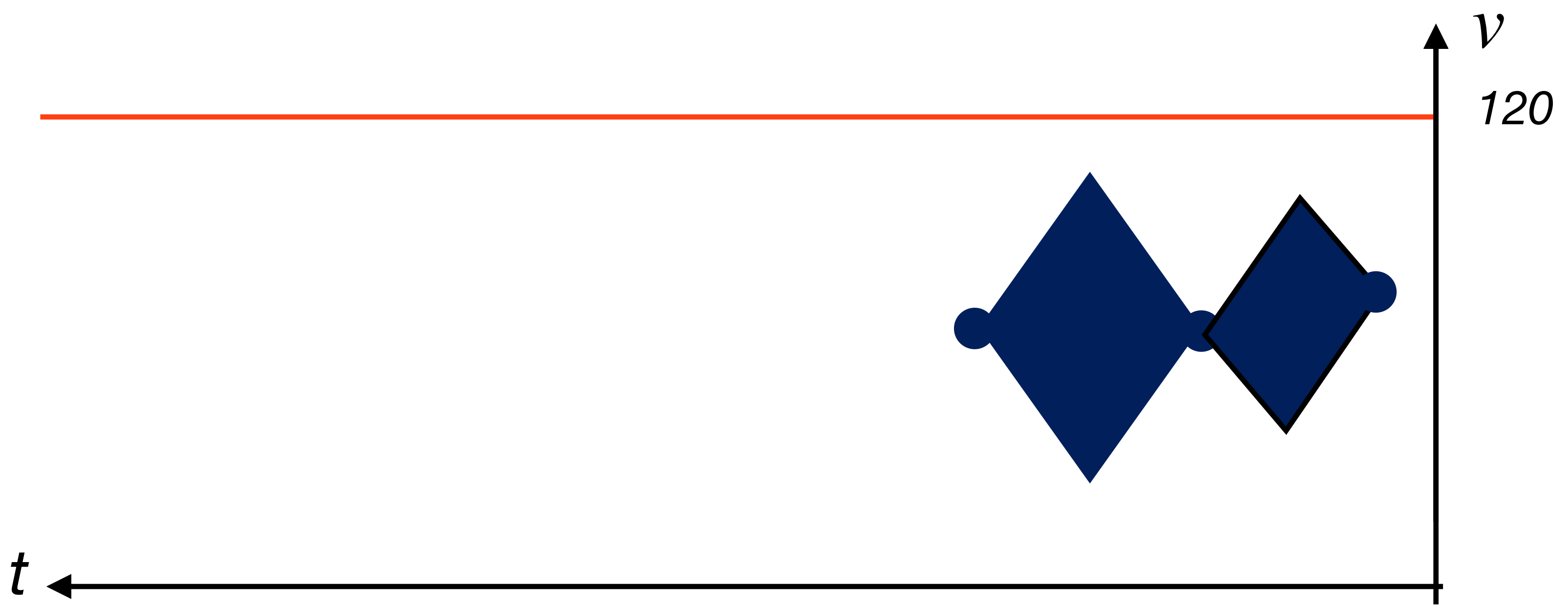
Algorithm: Bounded-time Reachability



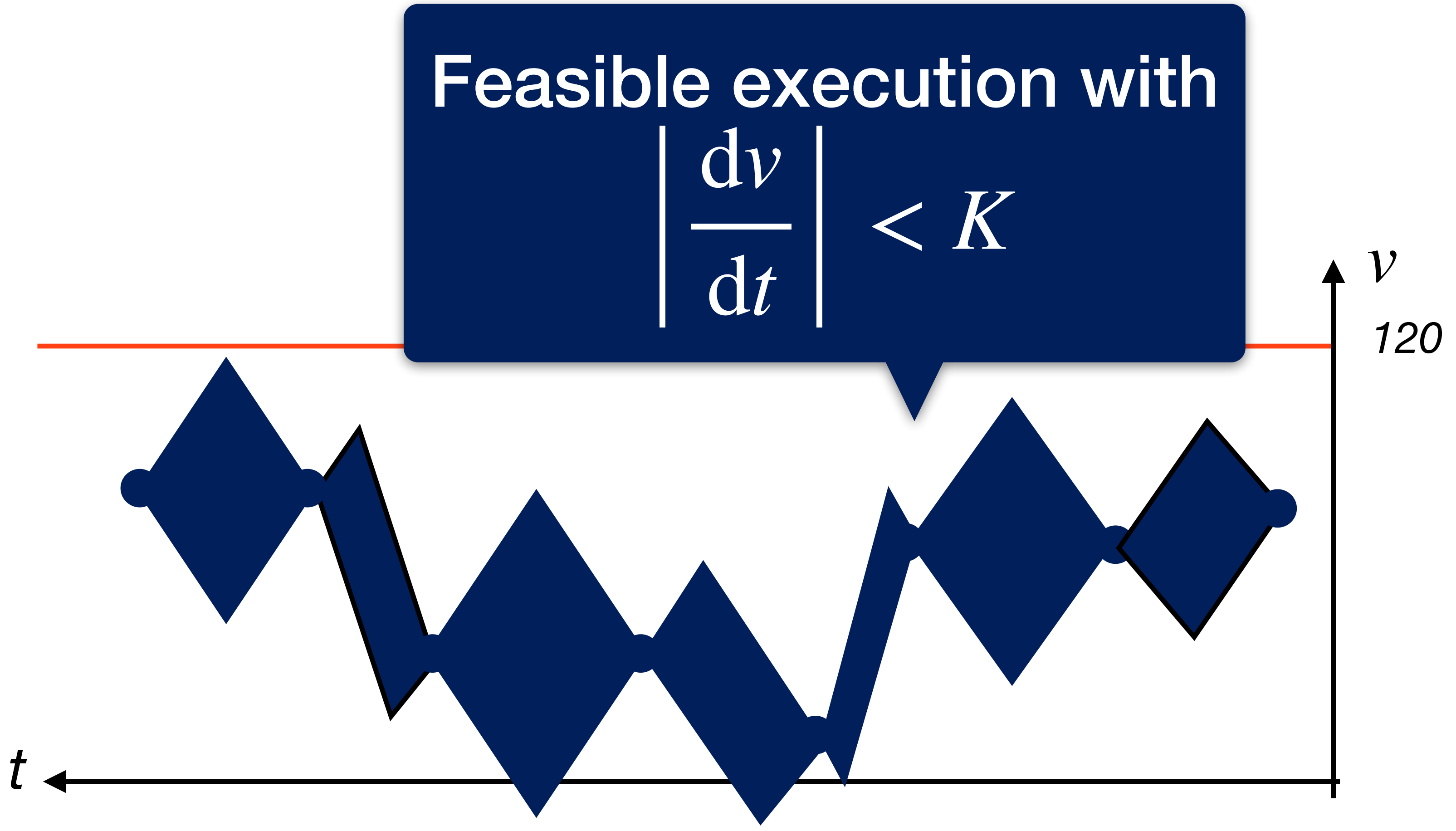
Algorithm: Bounded-time Reachability



Algorithm: Bounded-time Reachability

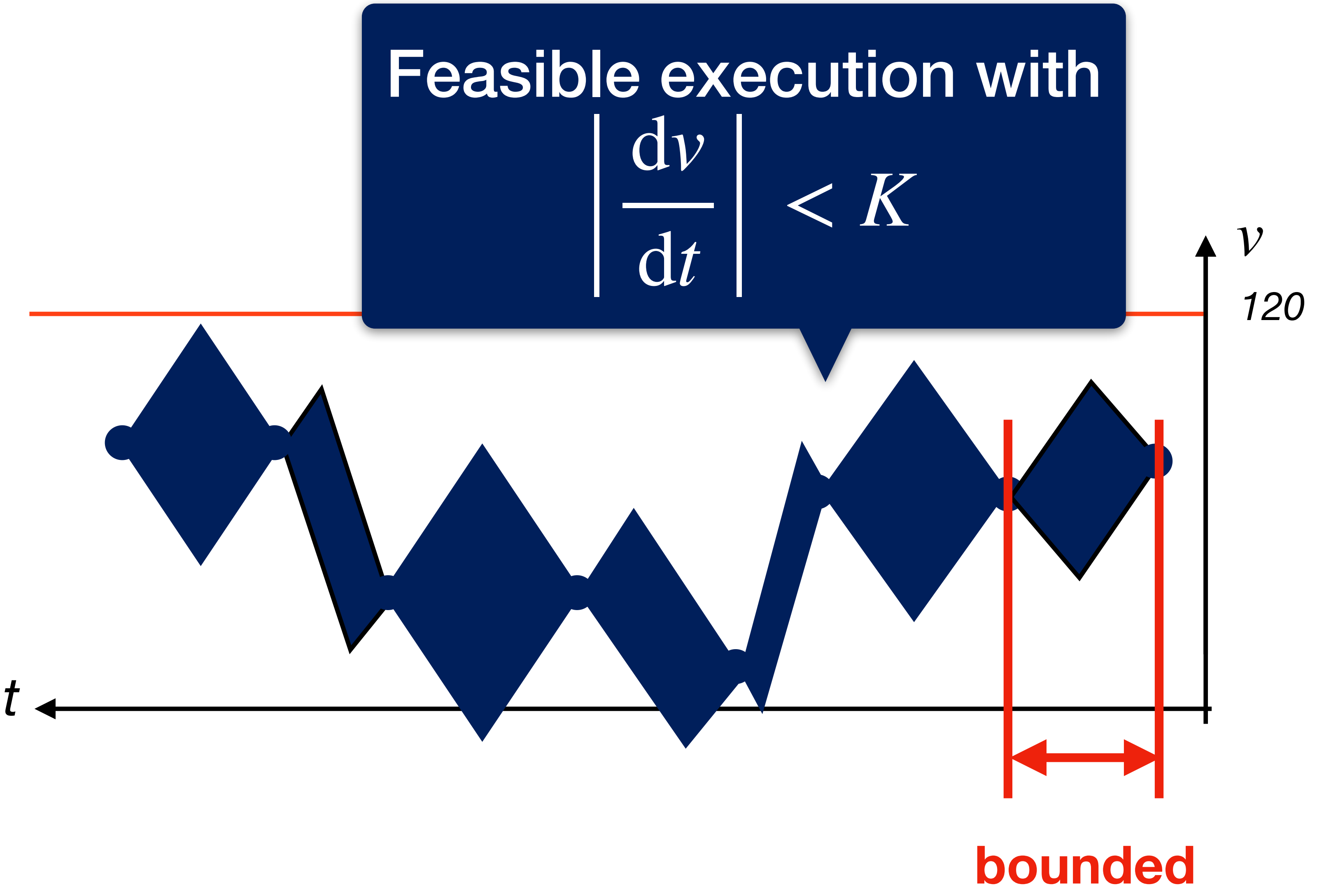


Algorithm: Bounded-time Reachability



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

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

Environment of Experiments

- Used 3 benchmarks on adaptive cruise controller (**ACC**) + 1 robot navigation (**NAV**) benchmark
- **ACC**: Cars should not be too close (or no physical contact)

For scalability analysis

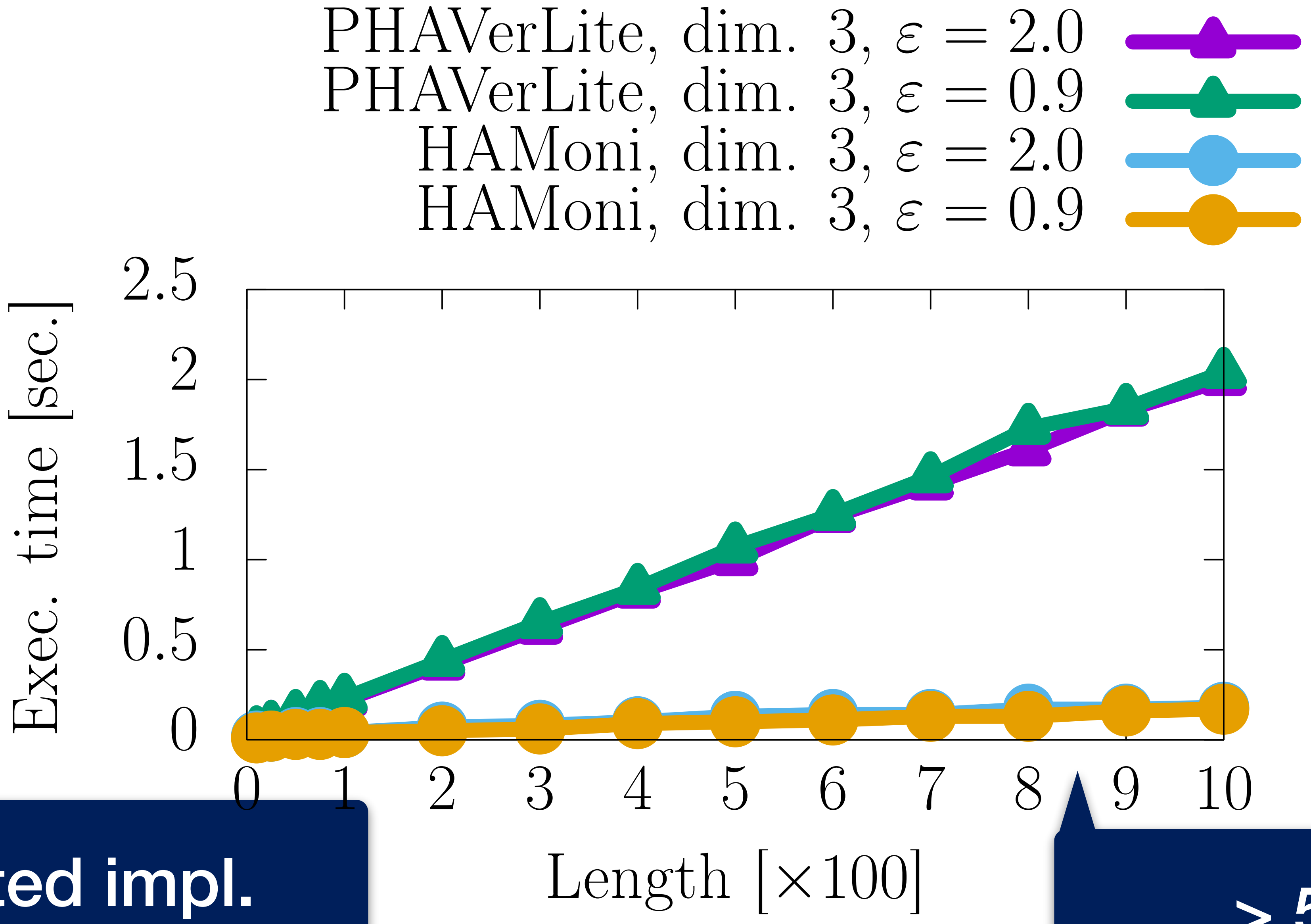
- **NAV**: Do not enter an unsafe region

For false alarms analysis

- Amazon EC2 c4.large instance / Ubuntu 18.04 LTS (64 bit)
  - 2.9 GHz Intel Xeon E5-2666 v3, 2 vCPUs, 3.75 GiB RAM

Experiment Results

Changing Observation Length

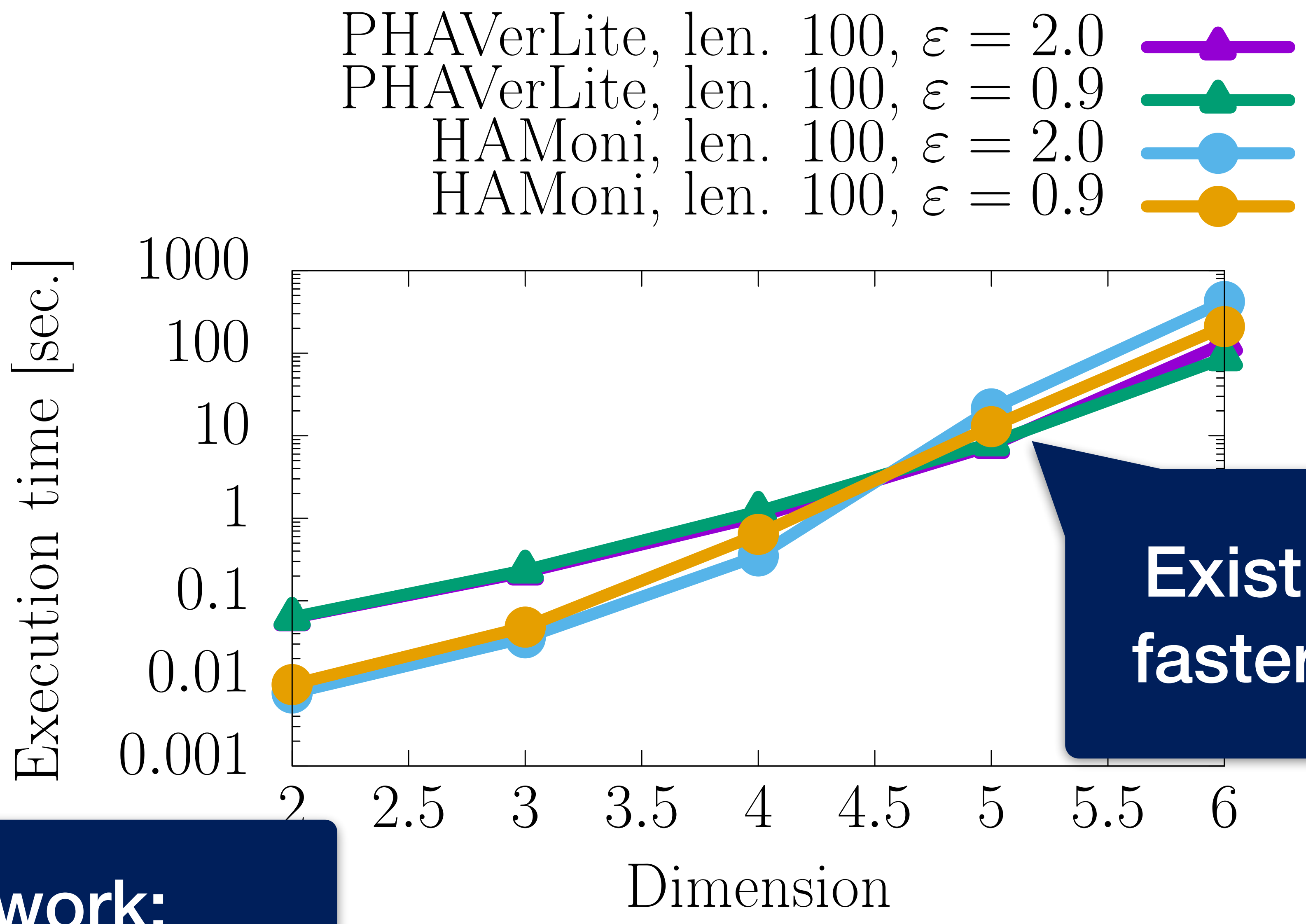


Dedicated impl.
≈ 10x faster

> 5000
samples / sec.

Experiment Results

Changing Model Dimension

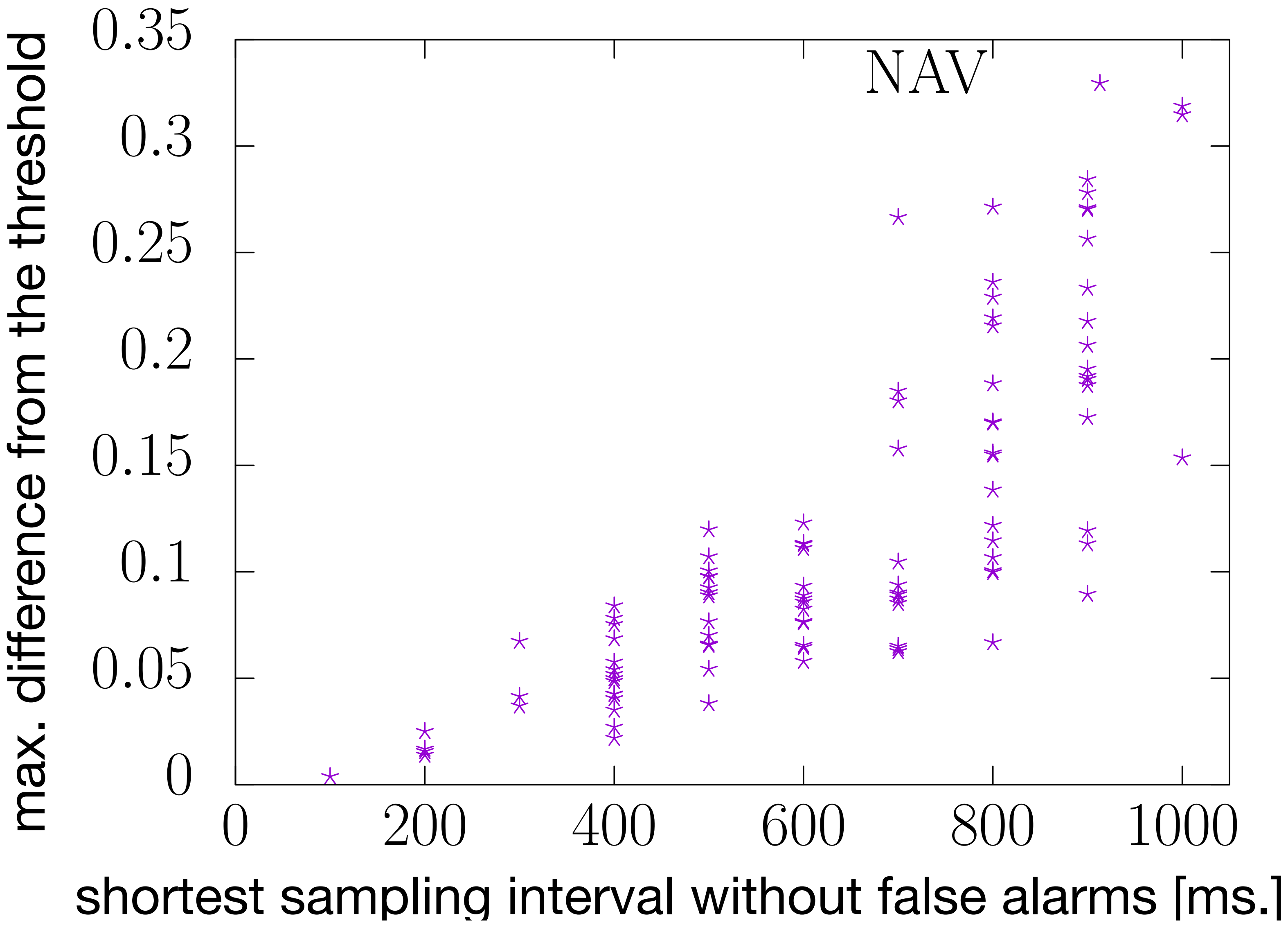


Existing tool was faster for dim. > 6

Future work: further optimization

Experiment Results

False Alarms



False alarm for “very safe” exec.
→ sampling is coarse

Conclusions

- Proposed model-bounded monitoring

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

- Formalized with monitored language $L_{\mathrm{mon}}(\mathscr{M})$

  $L_{\mathrm{mon}}(\mathscr{M})$: possible *discrete* observations of $\mathscr{M}$

- Algorithms + implementations

  Idea: bounded-time reachability
  Experiment → effectively monitorable