# Output-Feedback Safety-Preserving Control

M Yousefi[1], K van Heusden[1], **IM Mitchell**[2], GA Dumont[1]

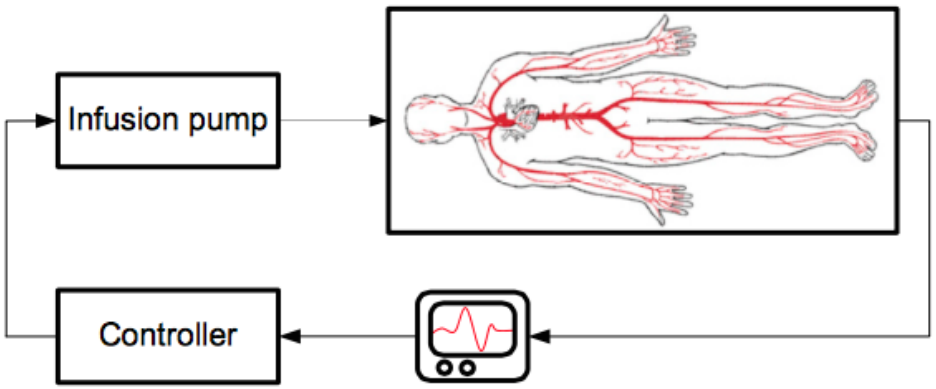
[1]Electrical and Computer Engineering Department
[2]Computer Science Department
The University of British Columbia

*Presented at ACC 2017*

May 2017

# Motivation

- Goal: deliver anesthetics to patients in closed-loop.
- Key element for FDA/Health Canada: guarantees of **safety**.



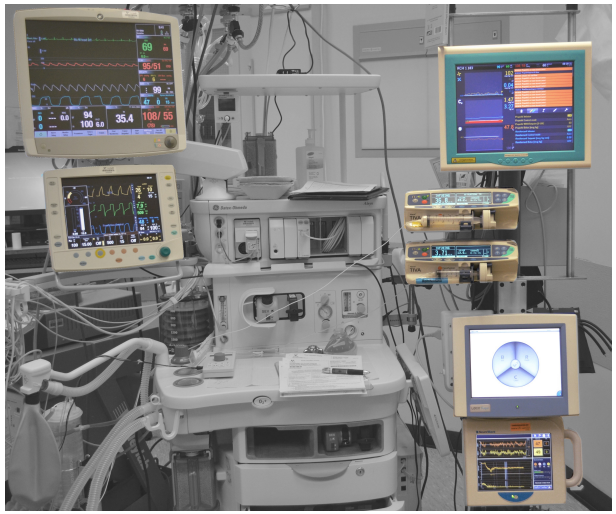
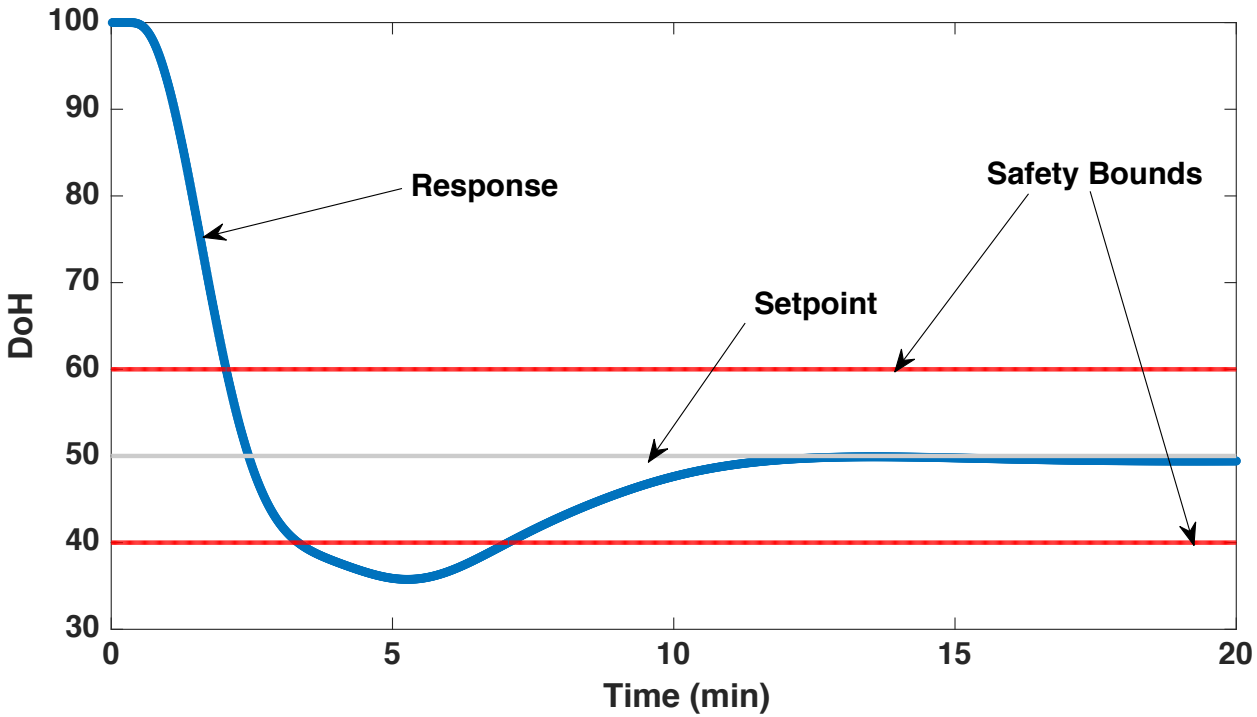



Figure: iControl

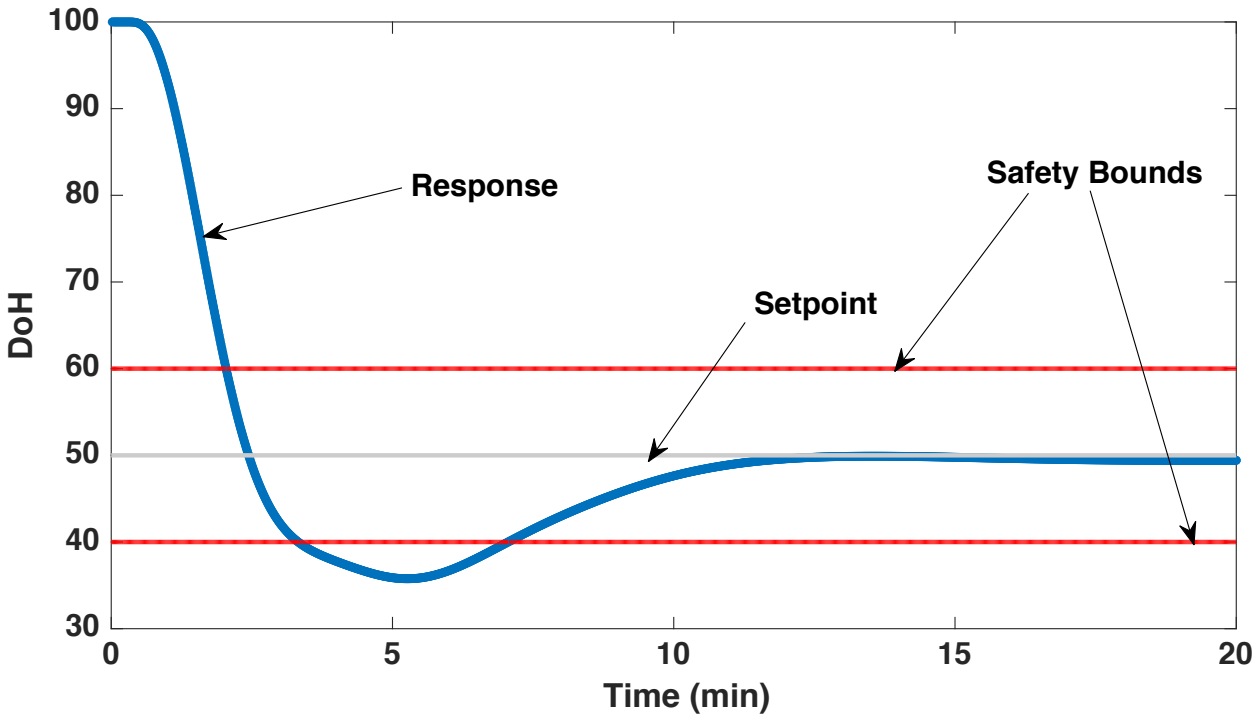
# Motivation

Example of an unsafe anesthesia response:



# Motivation

Example of an unsafe anesthesia response:



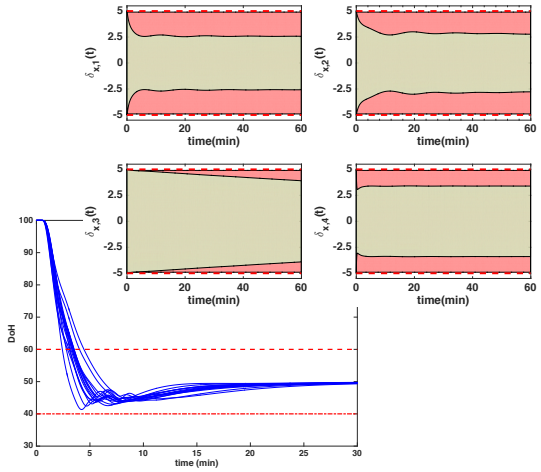

**Solution:**

Safety-preserving control and formal methods.

# Contributions

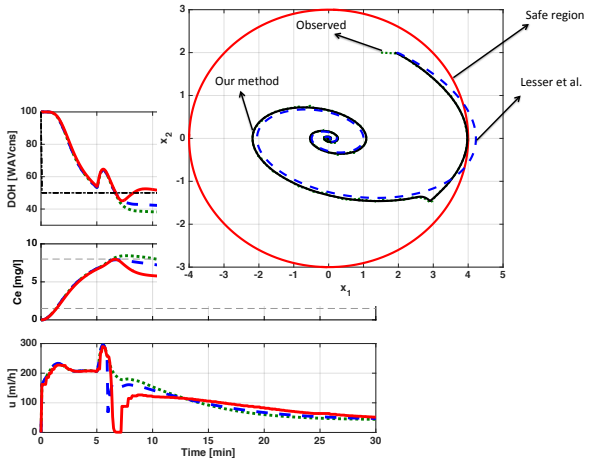
Theoretical:

- Safety in uncertain systems:
  - Yousefi et al., Model-invariant safety-preserving control, In ACC 2016.
  - Yousefi et al., Model-invariant viability kernel, Submitted to Automatica.
- Safety in output-feedback systems:
  - Yousefi et al., Output-feedback safety-preserving control, In ACC 2017.




Clinical:

- Yousefi et al., A formally verified safety system for closed-loop anesthesia, In IFAC WC 2017.
- Yousefi et al., Modelling blood pressure uncertainty for safety verification of propofol anesthesia, Submitted to SMC 2017.



# Contributions

**Paper's contribution:**

Guarantee safety of output-feedback systems.

Outline:

- Related work
- Problem formulation
- Output-feedback safety-preserving control
- Simulation results
- Conclusion

# Related Work

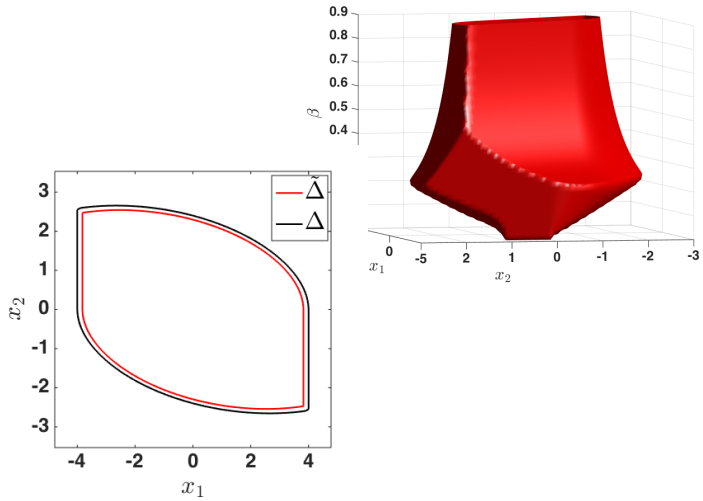
- Haesaert et al., Correct-by-design output feedback of LTI systems, In CDC 2015.
- Lesser et al., Safety verification of Output feedback controllers, In ECC 2016.

For example, Lesser et al.:

1. Design a high-gain observer,
2. Calculate a upper bound on the estimation error over all time,
3. Erode the safe region by the error upper bound,
4. Calculate the feedback invariant for the specified feedback controller.

This approach is:

- conservative,
- controller-specific,
- assumes initial error is zero.



# Our Approach

In this work, we:

1. Design a stable observer,
2. Formulate the error dynamics,
3. Calculate the error tube using the error dynamics,
4. Erode the safe tube by the error tube,
5. Synthesize an observer-based safety-preserving feedback controller envelope.

Our approach is:

- less conservative,
- not controller-specific.

# Problem Formulation & Assumptions

System Dynamics:

$$X: \quad \dot{x}_t = Ax_t + Bu_t, \quad y_t = Cx_t.$$
$$t \in \mathbb{T}, \quad x(\cdot) \in \mathcal{X}_{\mathbb{T}}, \quad u(\cdot) \in \mathcal{U}_{\mathbb{T}},$$

Observer:

$$O: \quad \dot{\hat{x}}_t = (A - LC)\hat{x}_t + Bu_t + LCx_t.$$

Assumptions:

- $(A, C)$ is observable,
- $L$ stabilizes $A - LC$.

Therefore, error $(e = x - \hat{x})$ dynamics is stable:

$$E: \quad \dot{e}_t = (A - LC)e_t.$$

# Definition

*Output-feedback safety preserving control* guarantees that

$$\exists u(\cdot) \in \mathcal{U}_{\mathbb{T}}, \quad s.t. \quad x(\cdot) \in \mathcal{X}_{\mathbb{T}},$$

despite the fact that $x(\cdot)$ is not measurable but is observable.

# Method

We calculate the evolution of the error dynamics (set of error trajectories):

$$\mathcal{E}_{\mathbb{T}} = \{e(\cdot) |\ \forall t \in \mathbb{T},\ e_t \in \mathcal{E}_t\}.$$

- Due to the stability of $(A - LC)$, $\mathcal{E}_t$ becomes smaller as $t$ goes forward.

The error dynamics can be reformulated as:

$$O: \quad \dot{\hat{x}}_t = A\hat{x}_t + Bu_t + LCe_t, \quad e_t \in \mathcal{E}_t.$$

Note:

- $\mathcal{E}_{\mathbb{T}}$ is a set of error trajectories.
- $\mathcal{E}_t$ is a set of states (errors) at time $t$.

# Method

Let's define $\hat{\mathcal{X}}_{\mathbb{T}}$ as:

$$\hat{\mathcal{X}}_{\mathbb{T}} = \mathcal{X}_{\mathbb{T}} \ominus \mathcal{E}_{\mathbb{T}},$$

We prove that if

$$\exists u(\cdot) \in \mathcal{U}_{\mathbb{T}} \implies \hat{x}(\cdot) \in \hat{\mathcal{X}}_{\mathbb{T}},$$

the same input keeps

$$x(\cdot) \in \mathcal{X}_{\mathbb{T}}.$$

So any safety-preserving controller that keeps $\hat{x}(\cdot) \in \hat{\mathcal{X}}_{\mathbb{T}}$, will keep the system safe.

# Method

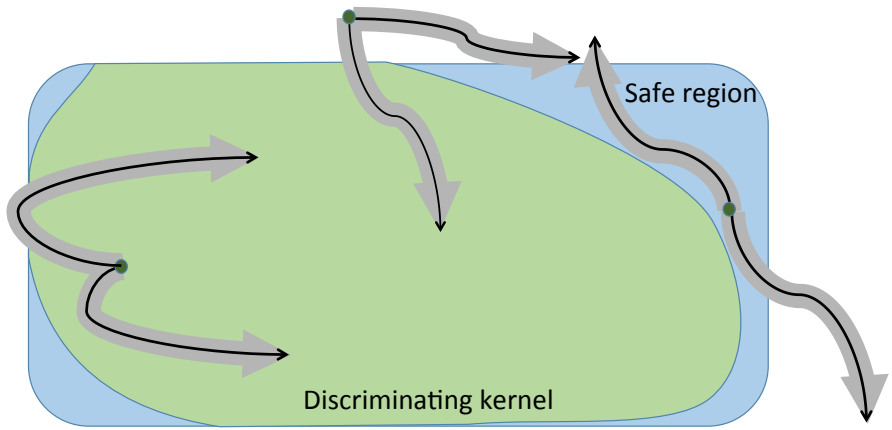
Reduced to already solved problem:

Step 1)

Discriminating kernel approximation for $\hat{x}(\cdot)$ dynamics.

Step 2)

Safety-preserving control synthesis



# Example

Double integrator[1] :

$$\begin{bmatrix} \dot{x}_1(t) \\ \dot{x}_2(t) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u(t),$$

$$y(t) = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix}.$$

$$|x_1(t)| \leq 4, \quad |x_2(t)| \leq 3, \quad |u(t)| \leq 1.$$

[1] Lesser et al., Safety verification of output feedback controllers for nonlinear system, In ECC 2016.

# Example

Double integrator:

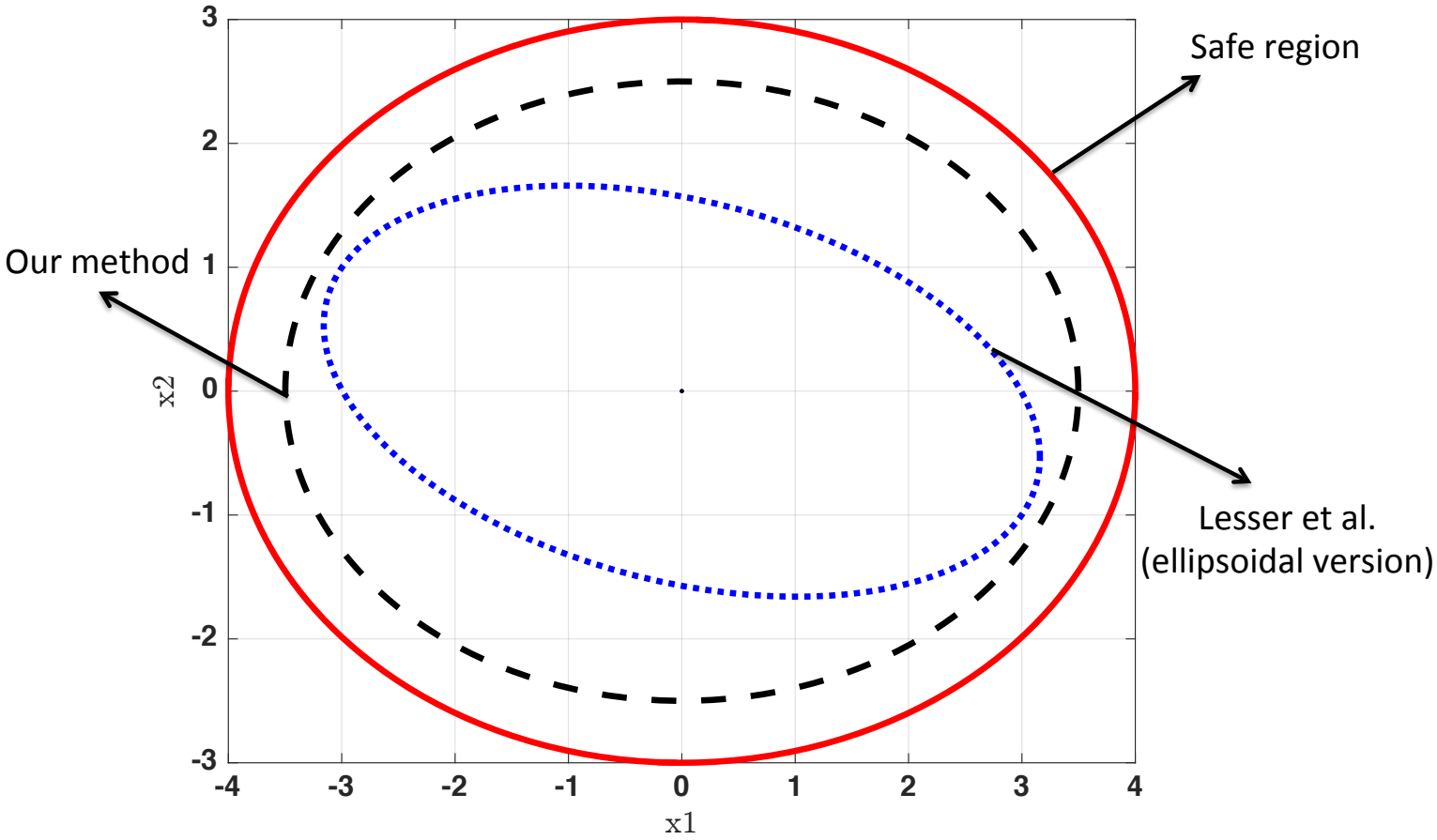



Figure: Viable sets for the double integrator at $t = 0$ ($\mathbb{T} = [0, 10s]$).

# Example

Double integrator:

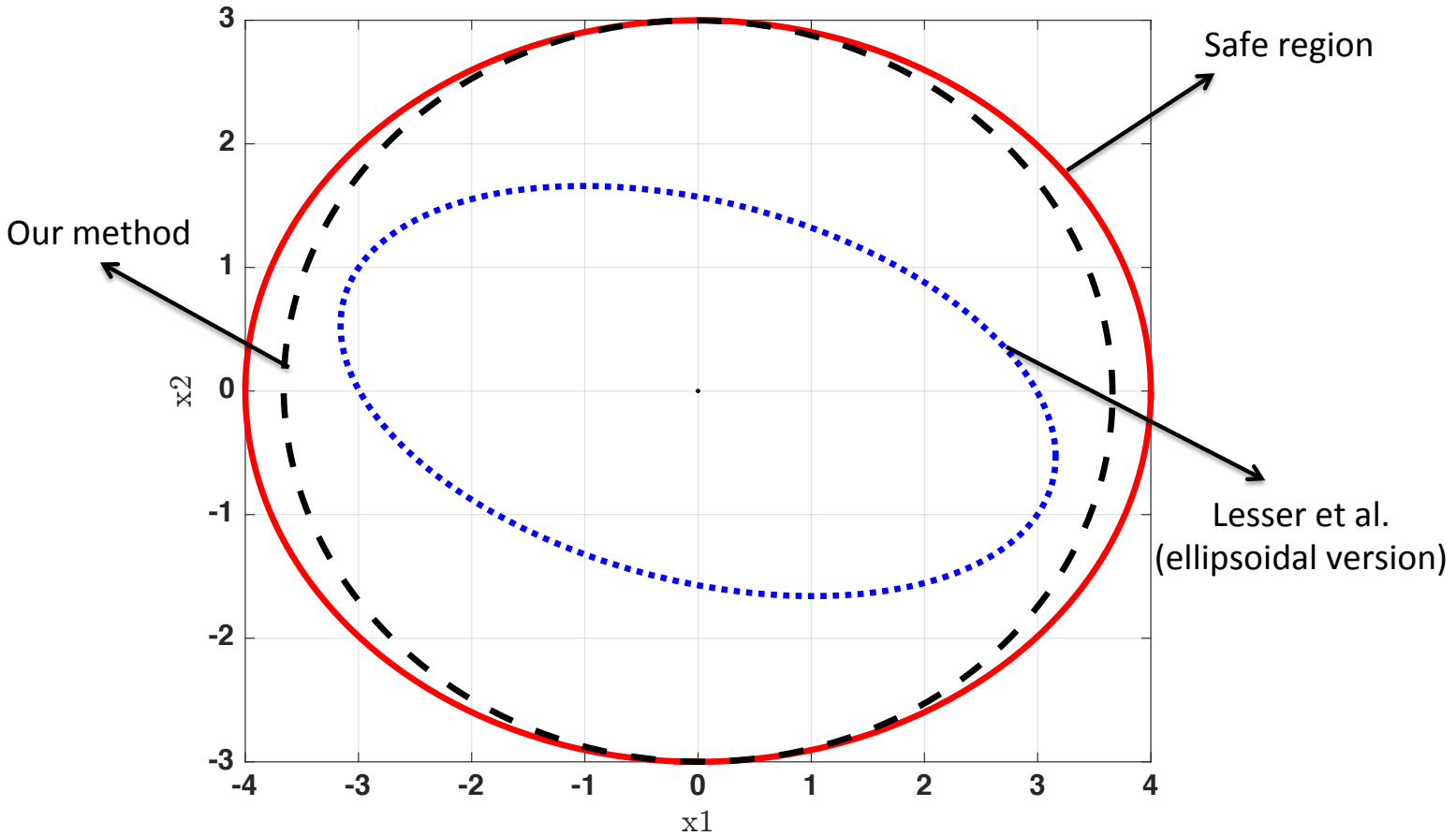



Figure: Viable sets for the double integrator at $t = 5s$ ($\mathbb{T} = [0, 10s]$).

# Example

Double integrator:

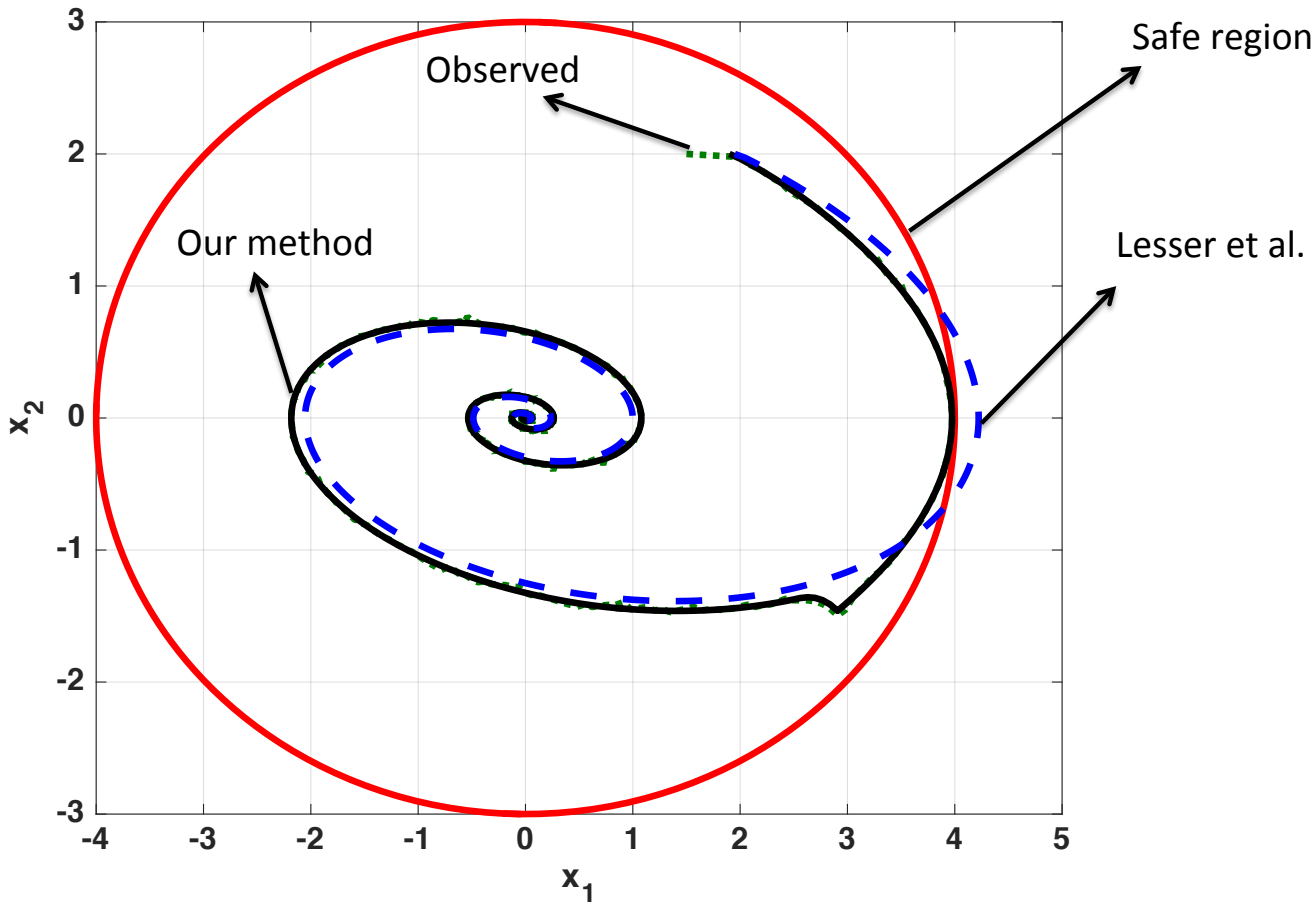



Figure: Closed-loop trajectories.

# Summary

Output-feedback safety-preserving scheme:

- Not controller-specific,
- Less conservative than Lesser et al.[2] ,
- Allows for non-zero initial conditions,
- Enables a variety of safety-preserving control schemes designed for fully observable systems.

Next step:

- Extend the proposed method to the case of
  - uncertain systems,
  - uncertain delays.

[2] Lesser et al., Safety verification of output feedback controllers for nonlinear system, In ECC 2016.

# Output-Feedback Safety-Preserving Control

M Yousefi, K van Heusden, IM Mitchell, GA Dumont

For more information:

mahdiyou@ece.ubc.ca (ece.ubc.ca/∼mahdiyou)
mitchell@cs.ubc.ca (cs.ubc.ca/∼mitchell)