

Aplicaciones de los Métodos Formales para una mayor Seguridad y Fiabilidad de Sistemas Ciber-Físicos

Marcelo Forets

Departamento de Matemática y Aplicaciones, CURE, Universidad de la República
Instituto Técnico Regional Centro-Sur, Universidad Tecnológica

Daniel Freire

Instituto de Física, Facultad de Ciencias, Universidad de la República

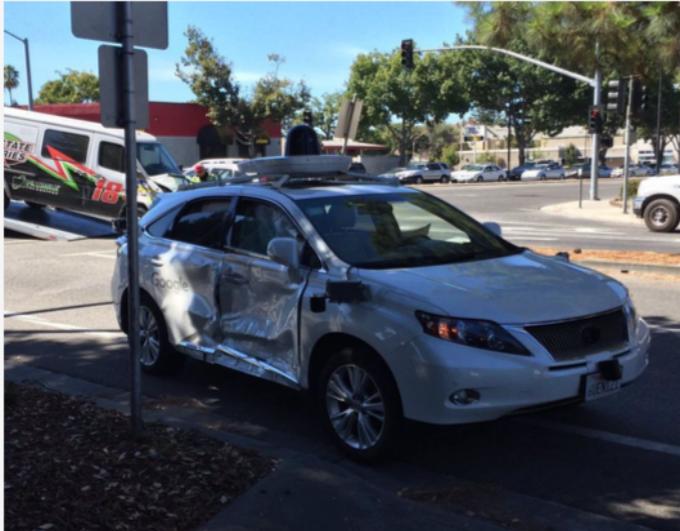
El Problema



Sistema ciber-físico: *todo aquél dispositivo que integra capacidades de computación para controlar e interactuar con un proceso físico.*

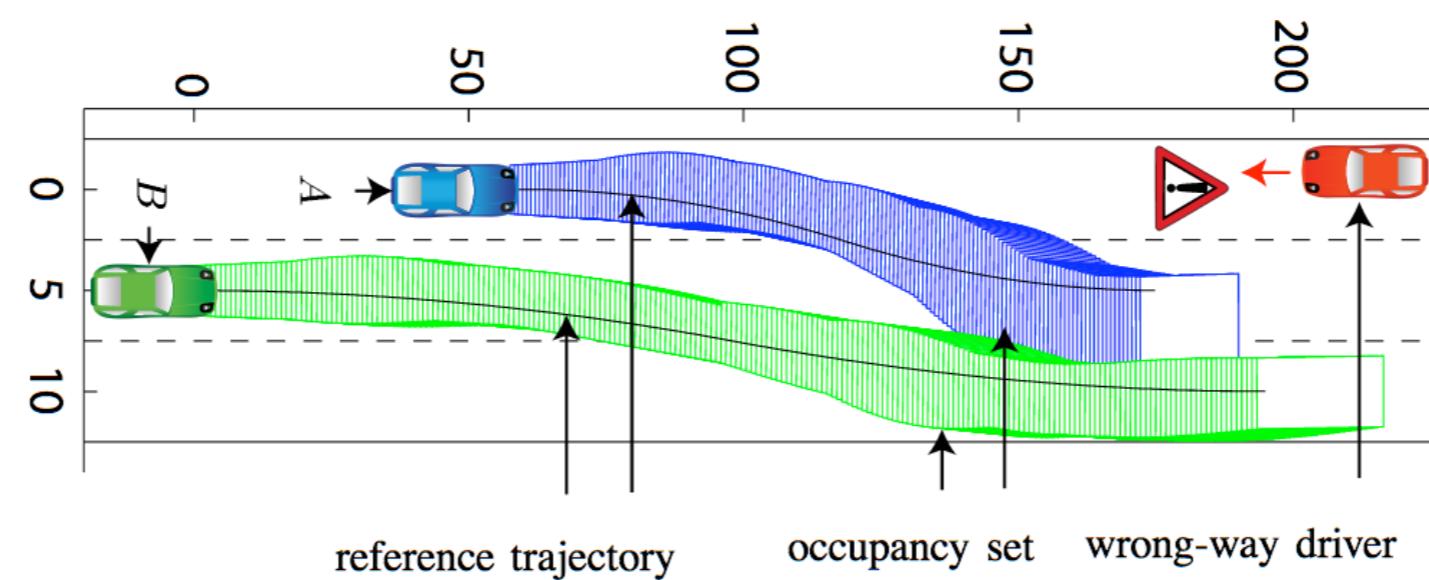
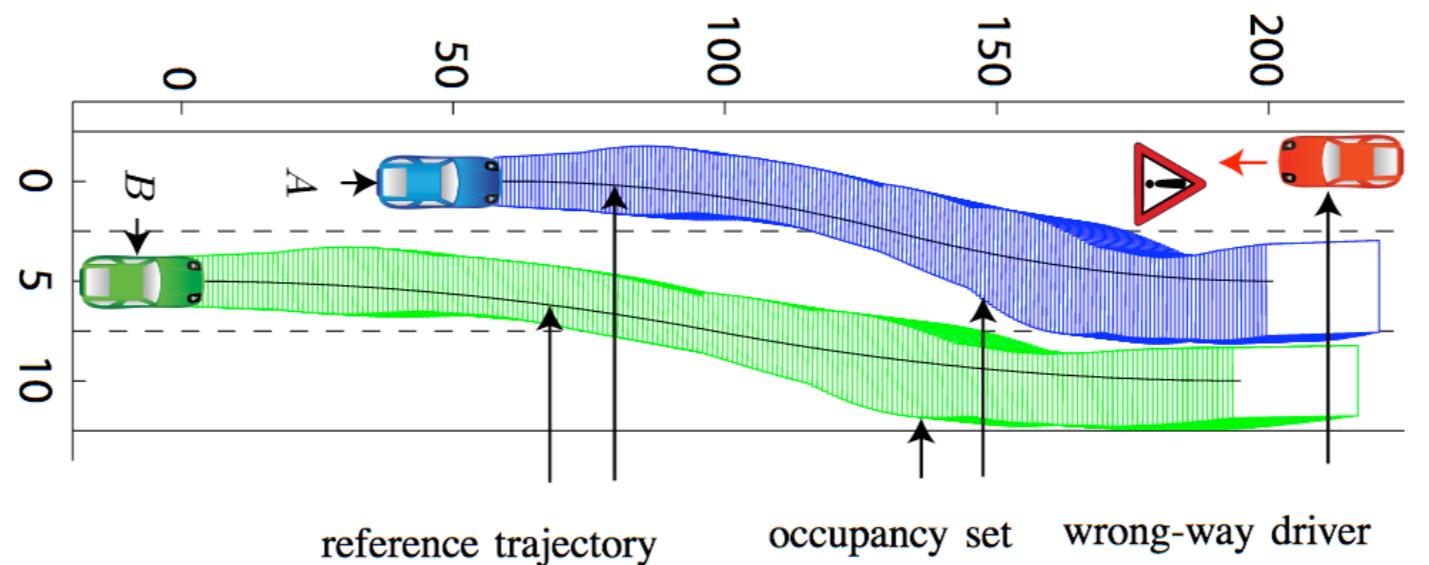
El Problema

Ejemplos de sistemas que no fueron verificados suficientemente:



Los métodos formales pueden dar garantías de **seguridad** y **fiabilidad** para los “sistemas críticos”.

EI Problema



El Problema

ARCH-COMP19 Category Report:
Continuous and Hybrid Systems with Nonlinear Dynamics

Fabian Immler¹, Matthias Althoff², Luis Benet³, Alexandre Chapoutot⁴, Xin Chen⁵, Marcelo Forets⁶, Luca Geretti⁷, Niklas Kochdumper², David P. Sanders⁸, and Christian Schilling⁹

¹ Computer Science Department, Carnegie Mellon University, United States
fimmler@cs.cmu.edu

² Technische Universität München, Munich, Germany
althoff@in.tum.de, niklas.kochdumper@tum.de

³ Instituto de Ciencias Físicas, Universidad Nacional Autónoma de México (UNAM), México
benet@icf.unam.mx

⁴ ENSTA ParisTech, Palaiseau, France
alexandre.chapoutot@ensta-paristech.fr

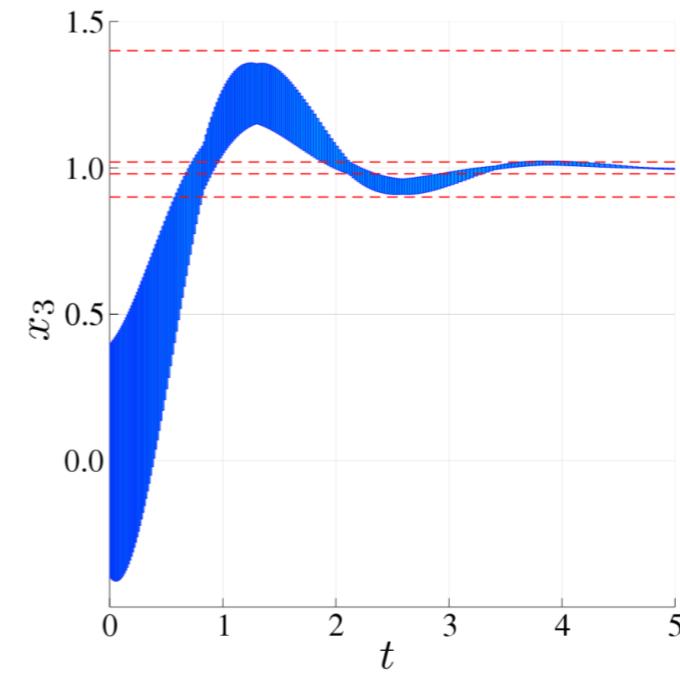
⁵ University of Dayton, Dayton, OH, United States
xchen4@udayton.edu

⁶ Universidad de la República, Uruguay
mforets@gmail.com

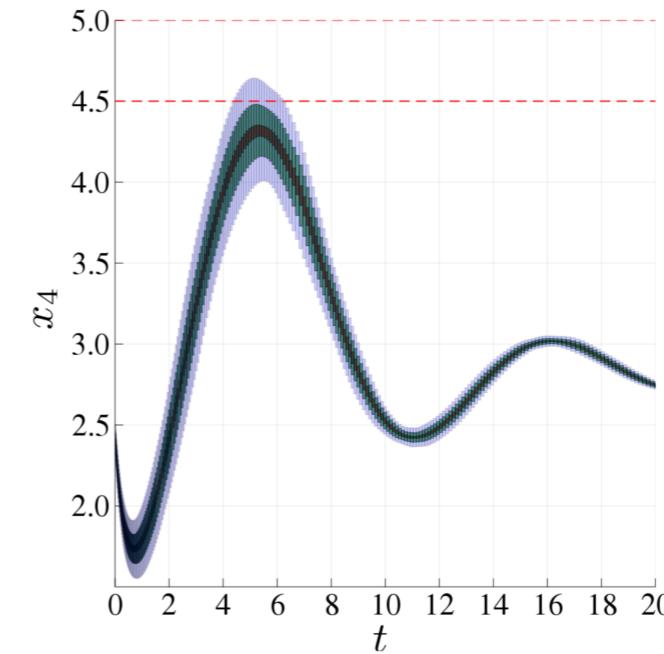
⁷ University of Verona, Verona, Italy
luca.geretti@univr.it

⁸ Departamento de Física, Facultad de Ciencias Físicas,
Universidad Nacional Autónoma de México (UNAM), México
dpsanders@ciencias.unam.mx

⁹ IST Austria, Klosterneuburg, Austria
christian.schilling@ist.ac.at



Control de altitud en un Quadrotor



Red molecular de proteínas
(Laub-Loomis)

La Idea

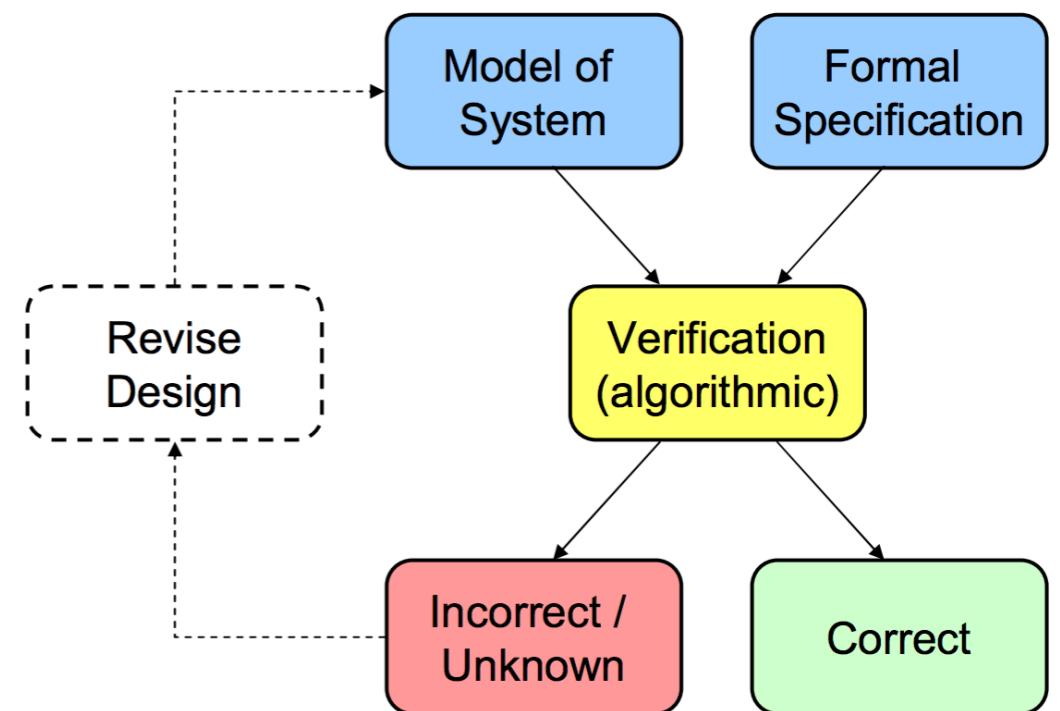
Desarrollar un servicio para el análisis de modelos utilizando métodos formales.

¿Qué es la verificación formal?

Dado el modelo de un sistema, verificar de forma automática y exhaustiva que éste cumple con determinada especificación.

(1) Análisis de alcanzabilidad

(2) Identificación de contraejemplos



Case Studies

[Filtered oscillator](#)[Cruise control](#)[Spacecraft
rendez-vous](#)[Quadrotor
stability control](#)[Laub-Loomis
molecule](#)[International
Space-Station](#)[Building](#)[3-vehicle platoon](#)

Structural model of component 1R (Russian service module) with 270 state variables

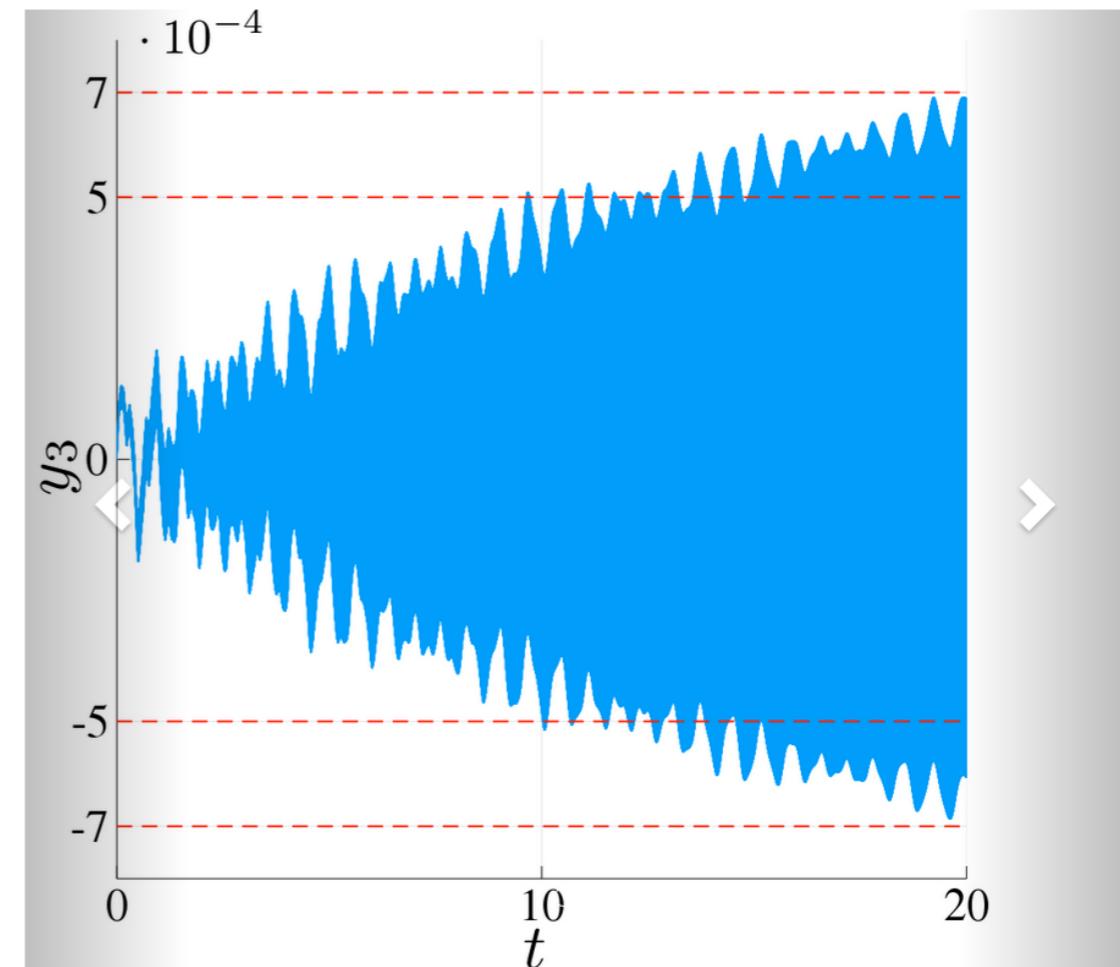
People

Developers

- [Marcelo Forets](#). Universidad de la República, Uruguay.
- [Kostiantyn Potomkin](#). Australian National University, Australia.
- [Christian Schilling](#). Institute for Science and Technology, Austria.

Scientific collaborators

- [Luis Benet](#). Instituto de Ciencias Físicas, Universidad Nacional Autónoma de México, México.
- [Sergiy Bogomolov](#). College of Engineering & Computer Science, Australian National University, Australia.
- [Goran Frehse](#). ENSTA ParisTech, France.
- [Andreas Podelski](#). University of Freiburg, Germany.
- [David P. Sanders](#). Departamento de Física, Facultad de Ciencias, Universidad Nacional Autónoma de México, México.
- [Frédéric Viry](#). CERFACS, France.



JuliaReach

Reachability Computations for Dynamical Systems in Julia

✉ <http://www.juliareach.org>