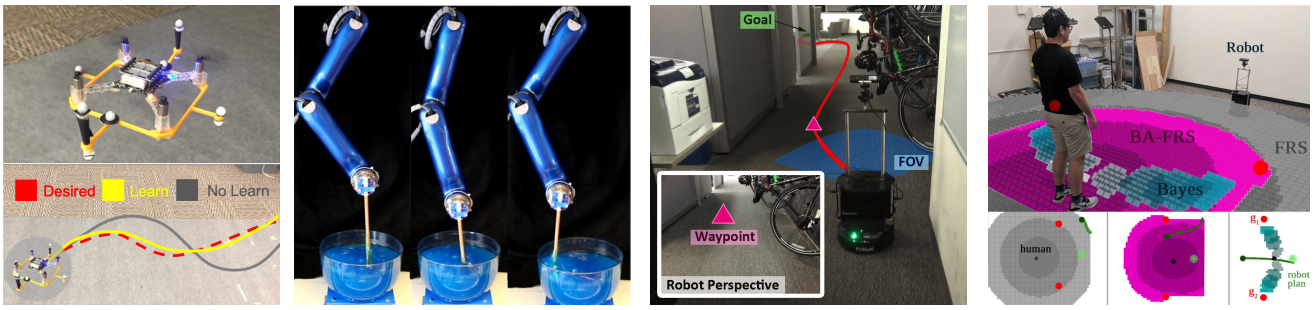
# Towards Safe and Intelligent Autonomy: A Control-Theoretic Approach to Learning and Perception

*Somil Bansal*

Machine learning has led to tremendous progress in domains such as computer vision, speech recognition, and natural language processing. Fueled by these advances, machine learning approaches are now being explored to develop intelligent physical systems that can operate reliably in unpredictable environments. These include not only robotic systems such as autonomous cars and drones, but also large-scale transportation and energy systems. However, learning techniques widely used today are extremely data inefficient, making it challenging to apply them to real-world physical systems. Moreover, they lack the necessary mathematical framework to provide guarantees on correctness, causing safety concerns as data-driven physical systems are integrated in our society.

To develop safe and intelligent systems, we should certainly leverage the adaptability of the modern data-driven approaches, but marry them with the classical approaches that have been used for decades to operate physical systems reliably in controlled environments. ***My research combines tools from robust optimal control theory with machine learning and computer vision to develop data-efficient and provably safe learning-based control algorithms for physical robotic systems.*** By combining system dynamics models with data, these algorithms learn to solve challenging perception and control problems in *a priori* unknown and hard-to-model environments in a *data-efficient* fashion. Crucially, models are used not only for faster learning, but also to actively reason about *safety* and take action to preserve it when necessary. The key novel contributions of my work are:

1) **Data-efficient task-based learning using models and optimal control:** developing optimal control-based learning frameworks for efficiently completing a given control task in hard-to-model environments [1]–[5].
2) **Data-efficient architectures for learning-based perception with model-based control:** developing perception-action loops that efficiently combine deep learning-based perception with an underlying dynamics model for control, such as to navigate in *a priori* unknown environments [6].
3) **Advancing the theory of optimal control for scalable safety analysis of learning-enabled systems:** introducing new formulations, theorems, and computational tools to enable run-time safety assurance for learning-enabled systems, including large-scale multi-agents systems [7]–[15].
4) **Safety assurance for learning-enabled systems in unknown and human-centric environments:** using the above tools to construct safety envelopes around learning-based perception and human motion prediction components, allowing robust motion plans to avoid collisions with obstacles and humans [16], [17].




(a) Data-efficient learning using optimal control to improve control performance in hard-to-model environments, e.g., (i) ground effects for quadrotors and (ii) fluid dynamics for jelly stirring task.

(b) Learning-based perception with model-based control for data-efficient navigation in unseen environments.

(c) Using models to provide safety guarantees around learning-based human motion predictors.

Fig. 1: My work develops data-efficient and provably safe learning-based control algorithms for physical robotic systems.

Together, these contributions enable data-efficient learning both for capturing external, hard-to-model environment effects, and for perception. Moreover, they allow for a safety analysis of the resulting learning-enabled systems. Achieving the objectives of my research has required bridging different areas of research. This goes beyond understanding the fundamentals of controller design and robustness in control theory [7]–[12], [18], [19] to its intersection

with computer vision, in collaboration with Jitendra Malik (UC Berkeley), Saurabh Gupta (UIUC) and Adam Bry (Skydio) [6]; formal methods, in collaboration with Sanjit Seshia (UC Berkeley) and Alberto Sangiovanni-Vincentelli (UC Berkeley) [14], [15]; and reinforcement learning and robotics, in collaboration with Sergey Levine (UC Berkeley), Anca Dragan (UC Berkeley), Roberto Calandra (Facebook Research) and Aleksandra Faust (Google Brain Robotics) [1]–[3], [17]. I have also connected these different communities through organizing workshops[1] and tutorials[2] at conferences, and seminars at UC Berkeley[3].

My research has also opened many promising future research directions. I will work on bridging the model-based and statistical verification techniques for ***scalable safety analysis of data-driven systems*** (Sec. II-A). I will work on ***robust integration between perception and control*** by using physical environment constraints to account for inaccuracies in perception systems (Sec. II-B). I will use model-based control not only for analysis, but also for actively gathering safety-critical data to ***design introspective learning-enabled systems for human-centric environments*** (Sec. II-C). Finally, I am excited to venture beyond navigation and develop ***general representations for interfacing perception and control*** for data-efficient control for other robotic tasks (Sec. II-D).

## I. Data-Efficient and Provably Safe Learning-Based Control for Physical Robotic Systems

### A. *Data-efficient task-based learning using models and optimal control*

Autonomous systems will inevitably experience external effects in unstructured environments, which are often hard to model using first principles. I have developed learning frameworks that leverage methods from system identification (SysID) and optimal control to efficiently capture these effects during the controller design process [1]–[4] (Fig. 1a). For example, I combined Bayesian optimization and optimal-control in closed-loop to develop aDOBO (Dynamics Optimization via Bayesian Optimization) [2], a framework for learning models of external effects that are specific to control task at hand. Unlike traditional SysID approaches, aDOBO does not necessarily find the most accurate dynamics model; instead, it learns a "coarse" model that can be learned with a small amount of data, and yet yields the best closed-loop controller performance when provided to the optimal control method used. I have collaborated with researchers at *TU Munich* to apply aDOBO to a 3-DoF robotic arm, which is tasked to stir jelly in a given pattern [4]. Rather than accurately modeling the complex nonlinear fluid dynamics, aDOBO leverages learning and optimal control for efficiently completing the task with a very high accuracy (Fig. 1a).

### B. *Data-efficient architectures for learning-based perception with model-based control*

In many applications of interest, simple and well understood dynamics models are sufficient for control, and it is rather the vision and perception components that require learning, such as to navigate in *a priori* unseen environments. Typically, a geometric map of the environment is used for navigation; however, real-time map generation can be challenging in texture-less environments or in the presence of transparent, shiny objects, or strong ambient lighting. In contrast, end-to-end learning approaches side-step this explicit map estimation step, but suffer from data inefficiency and lack of robustness. My factorized approach to robot navigation combine the generalization capabilities of deep learning-based perception with the robustness of model-based control [6]. More specifically, I trained a Convolutional Neural Network (CNN) that uses the RGB image observations to produce a sequence of intermediate *waypoints*, which are used as targets for a model-based optimal controller to generate smooth, dynamically feasible, and collision-free trajectories to be executed on the robot (Fig. 1b). Leveraging underlying dynamics and feedback-based control not only accelerate learning, but also leads to trajectories that are robust to variations in physical properties and noise in actuation. Through simulations and experiments on a mobile robot, I demonstrate that the proposed approach is *better* (45% more successful at reaching the goals), more *efficient* at reaching the goals (takes 35% less time), and results in *smoother* trajectories (56% less jerk), as compared to end-to-end learning. Due to the real-world imperfections in depth measurements, the proposed approach is more *reliable* (55% more successful) than geometric mapping-based approaches, as it does not explicitly rely on a map.

[1] 2019 RSS Workshop on Robust Autonomy: Safe Robot Learning and Control in Uncertain Real-World Environments
[2] 2017 CDC Tutorial on Hamilton-Jacobi Reachability: A Brief Overview and Recent Advances
[3] Design of Robotics and Embedded systems, Analysis, and Modeling Seminar (DREAMS)

Thanks to the presence of the visual and model-based feedback in the closed-loop, I demonstrate that the proposed approach can be *directly* transferred from simulation to unseen, real-world environments without any finetuning or data collection in the real-world (experiment videos on project website[4]). Although this work was only recently published, it has already shown promising impact: it has been highlighted in *Tech Xplore*[5], and has also sparked the interest of many ground and aerial vehicle companies, including *Skydio*, *Kiwi Campus*, *Ford*, *Nuro* and *Boeing*.

### C. *Advancing the theory of optimal control for scalable safety analysis of learning-enabled systems*

My work in Sec. I-A and I-B use models to develop data-efficient control mechanism both when learning is used for capturing unmodeled external effects or for perception. However, in addition to improving data-efficiency, the models can also be used to design learning-based systems that are analyzable. In my work, I use model-based Hamilton-Jacobi-Isaacs (HJI) reachability analysis for safe learning and exploration [10]. HJI analysis provides both the set of safe states and the corresponding safe controller for general nonlinear system dynamics. Since all system constraints are satisfied within this set, learning can be performed safely inside it. The main challenge is to scale HJI analysis to real-world autonomous systems because of its exponential computational complexity with respect to the number of state variables. In my work, I address this challenge on multiple fronts by leveraging (a) the structure in dynamics and control strategy [7]–[9], (b) offline computations [11], [12], and (c) modern computational tools [13] to perform this analysis tractably. For example, on the computation front, I introduced *BEACLS*, a C++-based reachability toolbox that can leverage modern computational tools such as GPUs to ***improve computation speed of HJI reachability by nearly 100 times*** compared to existing implementations [13]. On the algorithm front, rather than restarting the safety analysis from scratch, I proposed a method of "warm-start" reachability [12], which uses a user-defined initialization (typically a previously computed solution). By warm-starting an HJI value function, convergence may take significantly fewer iterations.

### D. *Safety assurance for learning-enabled systems in unknown and human-centric environments*

As the autonomous system is operating in its environment, it may experience changes in system dynamics or external disturbances, or it may evolve via learning-in-the-loop. Consequently, safety assurances need to be *evaluated* and *updated* at operation-time. This becomes particularly challenging when the system is operating in an unknown environment where even the unsafe states (such as obstacles) are not known *a priori*, such as navigation in an unseen environment. In such cases, rather than verifying the learning-enabled perception component explicitly, which can be quite challenging, I proposed an HJI reachability-based framework to compute and update a safe exploration region for the system. Within this region, learning can be performed without compromising safety.

Treating the unsensed environment as occupied, a safe region for the system is computed such that as long as the system is inside this set, it is guaranteed to avoid the collision regardless of the obstacle configuration in the unsensed environment [16]. This computation also provides a safe controller that can be combined with any optimistic planner, including learning-based planners, in a least-restrictive fashion, wherein the safety controller intervenes only when the safety is at risk. As the vehicle traverses through the environment, it explores the environment, and the safe region must be updated. Building on the scalable HJI analysis tools that I developed, I proposed a novel, real-time algorithm for updating the safe set to reflect this exploration. The proposed algorithm only *locally* updates the safe set in the newly sensed region while provably maintaining its conservativeness, significantly alleviating the computational burden of HJI reachability. I deployed the framework on a mobile hardware testbed that is using the learning-based perception-action loop discussed in Sec. I-B for navigation, but now also actively ensuring safety[6].

## II. Future research agenda

I envision future autonomous systems to be able to *introspect* and *reason* about the consequences of their actions, and use this information to *safely improve* over time to achieve their goals. A key step towards achieving this goal

[4] Project website: https://smlbansal.github.io/website-visual-navigation/

[5] Tech Xplore (WayPtNav: A new approach for robot navigation in novel environments)

[6] Experiment videos are on the project website: https://smlbansal.github.io/website-safe-navigation/

is to develop tools for scalable safety analysis of learning-enabled systems. I will bridge statistical and model-based approaches to reduce the computational complexity of verification methods. Furthermore, I plan to design robust perception systems that use tools from robust control to preemptively deal with prediction errors. I believe a symbiotic relationship between learning and control is required not only for safe control, but also to understand under what conditions the learning component leads to safety violations, and assisting it with collecting informative data samples in dynamic, human-centric environments. Finally, I will explore general representations between perception and control that allow the two to interface seamlessly for a variety of robotic and human-centric tasks.

### *A. Scalable safety analysis of data-driven systems*

I will continue to develop methods that can leverage the problem structure to achieve scalable safety analysis wherever possible, but I believe that for learning-enabled systems, we will need to bridge model-based analysis with statistical approaches for safety. Statistical approaches are naturally suitable for learning components that are inherently data-driven, whereas model-based approaches have been very successful for dynamical systems. At the expense of a small probability of failure, a rapprochement between the two has the potential to significantly alleviate the computational complexity of the safety analysis. Our preliminary results in [14] show that a sampling-based, data-driven approach can be combined with model-based analysis to provide strong probabilistic safety guarantees on the closed-loop system. I applied this framework for the safety analysis of a perception-action loop, designed for lane keeping for an autonomous car (Fig. 2). I plan to further explore these hybrid verification approaches for safety analysis of learning-enabled systems.

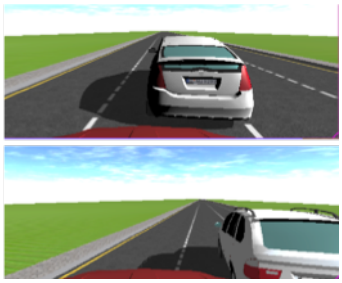


Fig. 2: Combining model-based and sampling-based methods for safety analysis. The framework can assess that a car in front or its shadow can occlude the lane, causing the failure of the perception module, and safety violation.

Much of my past work focuses on how to learn while satisfying safety constraints but less on developing learning approaches for safety. The same power of modern compute and data that is fueling perception can be leveraged to scale up verification and synthesis. This requires designing "correct-by-construction" learning components to avoid circular reasoning. There are some promising initial results in this direction [10] which I will investigate further in my group.

### *B. Robust integration between perception and control*

Learning-based perception components will inevitably have prediction errors. Moreover, imprecise real-world sensors will result in incomplete, inaccurate, and intermittent sensor data. From a control perspective, these can be treated as sensor errors that affect the feedback controller. I will work on tools from robust control to design feedback loops that are robust to such errors. I have taken some initial steps towards this direction where I model the prediction error of the perception component as a "disturbance" in the dynamical system and generate a waypoint that is robust to the worst-case disturbance. This preemptively provides a robustness margin for the perception module. I am very excited to explore these ideas further in the future. Moreover, my work so far primarily leverages a system model for designing robust learning-based controllers. However, physical environment constraints can also be used to increase the perception robustness. For example, a human on the road cannot be classified as a deer at the next time step if the perception system takes into account the implications of the dynamics constraints of the vehicle and the human on its scene. System dynamics and physical constraints naturally couple its actions and perception. I will leverage this coupling as a prior to develop robust perception systems for planning and control.

### *C. Designing introspective learning-enabled systems for human-centric environments*

When a system operates in dynamic environments, such as in the presence of humans, we need to preemptively understand how the system belief about the environment may change in light of data it is yet to observe. This self-assessment can be used not only for safeguarding against potential catastrophic changes in the system, but can also be a basis for active information gathering. For example, the realization that a narrow turn around the corner can lead to a collision with an unobserved pedestrian can be used to teach the system to make a wider turn and first examine

the intersection scenario. This active information gathering can ultimately enable self-diagnosis and self-repair in learning-enabled systems. I have recently embarked in this direction in [17] where I formulated the problem of finding all possible changes in the human behavior as a reachability problem. Possible future human observations are treated as 'input' to a dynamical system, and how the belief over human intention changes based on the data are the 'dynamics' of the system. Preliminary simulations and experiments indicate that this introspective nature of the human motion predictor with respect to the unobserved data enables safe planning around humans while being resilient to the changes in the data-driven predictive model (Fig. 1c). I will continue to work in this direction, particularly on how these techniques can be used for active information gathering about humans.

### *D. General representations for interfacing perception and control*

One important question that needs to be addressed to develop frameworks that seamlessly combine perception and control is "what is the right representation to interface perception and control?" For example, a mobile robot might need to open doors on its way to goal. The waypoint representation used in my work to interface perception and control may not be sufficient for opening doors. I would like to explore the use of hybrid systems theory within this context, where multiple different interfaces exist between perception and control, and the system will reason about how to switch between these interfaces to achieve its goal. Another direction that I am very excited about is to *learn* the correct representations between perception and control. As a first step towards this, I have started a collaboration with visual neuroscientists at UC Berkeley where we are trying to understand the kind of representations humans use to solve different tasks flexibly.

## III. Prospective Lab, Collaborations, and Funding

**Collaborations.** My work on combining deep learning-based perception with model-based control has sparked the interest of many aerial vehicle companies (*Skydio* and *Boeing*), ground vehicle companies (*Kiwi Campus*), autonomous driving companies (*Ford*, *Nuro* and *Toyota research*), industrial research labs (*DeepMind*, *Facebook research*, *Google Brain Robotics*), and various academic research labs. My safe multi-vehicle trajectory planning work has helped in shaping NASA's paradigm for integrating unmanned aerial vehicles into the national airspace. More generally, my work has immediate connections with the domains of control, formal methods, computer vision, reinforcement learning, robotics, and human-robot interaction. I look forward to continuing these collaborations, but am also very excited to cultivate new ones. The proposed paradigms for integrating vision and control can help in designing similar paradigms for general perception modalities, such as sound, language, and touch. At the core, I study how learning and models should be combined together to make efficient and safe decisions. The obtained insights can also be applied to general learning-enabled physical systems, such as transportation and energy systems. In particular, my prior work on energy systems [18], [19] has left me with a lasting interest in this domain, which I would like to explore further. Finally, I look forward to drawing inspiration from findings in cognitive science to develop truly versatile and intelligent systems.

**Lab.** I plan to set up a lab ramping up to a size of 6-8 researchers (graduate students and postdocs). My lab will be uniquely positioned not only to construct sound theoretical guarantees for autonomous systems, but also to carry out hardware experiments to establish their validity in real robotic systems. An ideal starting space would consist of office space and lab space dedicated to robotic testbeds. Equipment will include a motion capture area, a number of quadrotors and true to scale ground vehicles, a dynamic legged robot, and a robotic arm.

**Funding.** Developing safe and intelligent autonomous systems is an important research agenda of various funding programs, such as the Machine Learning, Reasoning and Intelligence program at ONR, and the Smart and Autonomous Systems program at NSF. During my PhD studies, I have made significant contributions to successful proposals for both funding agencies and industry. For example, I wrote the proposal for the *Google Commons* program, and co-wrote proposals for the *DARPA Assured Autonomy* program and the *NSF Frontier: VeHICal* project. Other than contributing to grant proposals, I have also actively participated in research discussions with the corresponding program managers. My research work can also be funded through industry. I will build upon my ongoing collaborations with companies such as Google Robotics, Boeing, and Toyota, and foster new ones.

## REFERENCES


[1] **S. Bansal**, A. K. Akametalu, F. J. Jiang, F. Laine, and C. J. Tomlin, "Learning quadrotor dynamics using neural network for flight control," in *IEEE Conference on Decision and Control (CDC)*, 2016.

[2] **S. Bansal**, R. Calandra, T. Xiao, S. Levine, and C. J. Tomlin, "Goal-driven dynamics learning via Bayesian optimization," in *IEEE Conference on Decision and Control (CDC)*, 2017.

[3] **S. Bansal**, R. Calandra, K. Chua, S. Levine, and C. Tomlin, "MBMF: Model-based priors for model-free reinforcement learning," *arXiv preprint*, 2017.

[4] T. Beckers, **S. Bansal**, C. J. Tomlin, and S. Hirche, "Closed-loop model selection for kernel-based models using Bayesian optimization," in *IEEE Conference on Decision and Control (CDC)*, 2019.

[5] **S. Bansal** and C. J. Tomlin, "Control and safety of autonomous vehicles with learning-enabled components," in *Safe, Autonomous and Intelligent Vehicles*. Springer, 2019, pp. 57–75.

[6] **S. Bansal**, V. Tolani, S. Gupta, J. Malik, and C. Tomlin, "Combining optimal control and learning for visual navigation in novel environments," in *Conference on Robot Learning (CoRL)*, 2019.

[7] M. Chen, S. L. Herbert, M. S. Vashishtha, **S. Bansal**, and C. J. Tomlin, "Decomposition of reachable sets and tubes for a class of nonlinear systems," *IEEE Transactions on Automatic Control (TAC)*, vol. 63, no. 11, pp. 3675–3688, 2018.

[8] **S. Bansal**, M. Chen, J. F. Fisac, and C. J. Tomlin, "Safe sequential path planning under disturbances and imperfect information," in *American Control Conference (ACC)*, 2017.

[9] M. Chen, **S. Bansal**, J. F. Fisac, and C. J. Tomlin, "Robust sequential trajectory planning under disturbances and adversarial intruder," *IEEE Transactions on Control Systems Technology (TCST)*, no. 99, pp. 1–17, 2018.

[10] **S. Bansal**, M. Chen, S. Herbert, and C. J. Tomlin, "Hamilton-Jacobi reachability: A brief overview and recent advances," in *IEEE Conference on Decision and Control (CDC)*, 2017.

[11] S. L. Herbert, M. Chen, S. Han, **S. Bansal**, J. F. Fisac, and C. J. Tomlin, "FaSTrack: a modular framework for fast and guaranteed safe motion planning," in *IEEE Conference on Decision and Control (CDC)*, 2017.

[12] S. L. Herbert, **S. Bansal**, S. Ghosh, and C. J. Tomlin, "Reachability-based safety guarantees using efficient initializations," in *IEEE Conference on Decision and Control (CDC)*, 2019.

[13] **S. Bansal**, M. Chen, K. Tanabe, and C. J. Tomlin, "Provably safe and scalable multi-vehicle trajectory planning," *IEEE Transactions on Control Systems Technology (TCST), under review*.

[14] S. Ghosh, **S. Bansal**, A. Sangiovanni-Vincentelli, S. A. Seshia, and C. J. Tomlin, "A new simulation metric to determine safe environments and controllers for systems with unknown dynamics," in *ACM International Conference on Hybrid Systems: Computation and Control (HSCC)*, 2019.

[15] **S. Bansal**, S. Ghosh, A. Sangiovanni-Vincentelli, S. A. Seshia, and C. J. Tomlin, "Context-specific validation of data-driven models," *arXiv preprint*, 2018.

[16] A. Bajcsy, **S. Bansal**, E. Bronstein, V. Tolani, and C. J. Tomlin, "An efficient reachability-based framework for provably safe autonomous navigation in unknown environments," in *IEEE Conference on Decision and Control (CDC)*, 2019.

[17] **S. Bansal**, A. Bajcsy, E. Ratner, A. D. Dragan, and C. J. Tomlin, "A Hamilton-Jacobi reachability-based framework for predicting and analyzing human motion for safe planning," in *International Conference on Robotics and Automation (ICRA)*, 2019 (*under review*).

[18] **S. Bansal**, M. N. Zeilinger, and C. J. Tomlin, "Plug-and-play model predictive control for electric vehicle charging and voltage control in smart grids," in *IEEE Conference on Decision and Control (CDC)*, 2014.

[19] C. Le Floch, **S. Bansal**, C. J. Tomlin, S. J. Moura, and M. N. Zeilinger, "Plug-and-play model predictive control for load shaping and voltage control in smart grids," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2334–2344, 2017.