Many cyber-physical systems (like planes, trains and self-driving cars) are safety critical but difficult to reason about. Formal verification can provide strong safety guarantees, but most industrial controllers are too complex to formally verify. *Safe control envelopes* characterize families of safe controllers and are used to monitor untrusted controllers at runtime [7]. They can put complex controllers, even when machine learning based [3], within the reach of formal guarantees because they model verifiable *abstractions* of control systems that isolate the parts relevant to safety without the full complexity of a specific control implementation. My research interests lie in the design of safe control envelopes. Verified safe control envelopes are hard to design, requiring domain expertise, many engineering hours and complex mathematical reasoning. My work seeks to (1) lower manual effort by providing synthesis techniques to automate the control envelope design process and (2) scale envelopes to harder problems by solving challenging case studies and generalizing the resulting insights.

When designing control envelopes, engineers are good at specifying the *shape* of a model and listing the possible control actions by translating client specifications. But identifying the exact control conditions required for safety in a model is a much harder problem that requires design insights and creativity, and is the main point of the deep area of control theory. Our algorithm CESAR [4] addresses this problem by filling in the holes of a hybrid systems model to identify a correct-by-construction control envelope, providing the first approach to symbolic control envelope synthesis. Existing controller synthesis techniques do not solve control *envelope* synthesis because control envelopes have the higher order constraint of permitting as many valid control solutions as possible, which does not, e.g., fit in the CEGIS [8] quantifier alternation pattern. The central insight of CESAR is that an optimal solution to the synthesis problem can be implicitly characterized via hybrid games, and these games can be solved to obtain an explicit solution via symbolic execution and systematic game refinements. My current work generalizes this approach. It identifies an implicit game characterization of control envelope synthesis solutions for a broad class of systems. To extract an explicit solution from these characterizations, it seeks to develop a domain-specific language that allows users to provide the human-intuition-based insights that, together with automated reasoning, can complete the control envelope synthesis process.

Our challenging control envelope synthesis case study [6] creates the first train control envelope that accounts for all the forces in the realistic Federal Railroad Authority Train Kinematics Model [1]. The competing physical effects of rolling resistance, track slope, curve resistance, and air brake propagation time interact subtly resulting in complicated dynamics. As a consequence, designing a controller with confidence that it is safe in every situation is hard. We used formal verification to design a trustworthy control envelope. I wrote mechanized proofs of correctness in CPS theorem prover KeYmaera X [2] that are available online [5]. The system posed several challenges – quantities unknown at proof time (the slope and curve profile of the track), cyclic interdependence between system variables, piecewise function behavior, and transcendental dynamics. I developed generalizable techniques to overcome them. I am currently formalizing the handling of cyclic interdependence between system variables as an algorithm that generates provably correct symbolic bounds on interdependent variables in time triggered controllers (where the controller takes a decision repeatedly with some maximum latency).

References

[1] Joseph Brosseau and Bill Moore Ede. Development of an adaptive predictive braking enforcement algorithm. Technical Report FRA/DOT/ORD-9/13, Federal Railroad Administration, 2009.

[2] Nathan Fulton, Stefan Mitsch, Jan-David Quesel, Marcus Völp, and André Platzer. KeYmaera X: An axiomatic tactical theorem prover for hybrid systems. In *CADE*, pages 527–538, 2015.

[3] Nathan Fulton and André Platzer. Safe reinforcement learning via formal methods: Toward safe control through proof and learning. In *Proceedings of the Thirty-Second AAAI Conference on Artificial Intelligence and Thirtieth Innovative Applications of Artificial Intelligence Conference and Eighth AAAI Symposium on Educational Advances in Artificial Intelligence*, AAAI'18/IAAI'18/EAAI'18. AAAI Press, 2018.

[4] Aditi Kabra, Jonathan Laurent, Stefan Mitsch, and André Platzer. CESAR: Control envelope synthesis via angelic refinements. In Laura Kovacs and Bernd Finkbeiner, editors, *TACAS*, LNCS. Springer, 2024.

[5] Aditi Kabra, Stefan Mitsch, and Andre Platzer. Verified Train Controllers for the Federal Railroad Administration Train Kinematics Model: Balancing Competing Brake and Track Forces (Models and Proofs). 8 2022.

[6] Aditi Kabra, Stefan Mitsch, and André Platzer. Verified train controllers for the federal railroad administration train kinematics model: Balancing competing brake and track forces. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 41(11):4409–4420, 2022.

[7] Stefan Mitsch and André Platzer. Modelplex: verified runtime validation of verified cyber-physical system models. *Formal Methods Syst. Des.*, 49(1-2):33–74, 2016.

[8] Armando Solar-Lezama. Program sketching. *STTT*, 15(5-6):475–495, 2013.

Curriculum Vitae

Education

Candidate for PhD in Computer Science, Carnegie Mellon University, Pittsburgh, PA, USA

Fall 2020 – present.
Advisors: André Platzer and Stefan Mitsch.

Bachelor of Science, Cornell University, Ithaca, NY, USA

Fall 2016 – Fall 2019.
magna cum laude in Computer Science, *cum laude* in Mathematics, *cum laude* in Physics.

Publications

- CESAR: Control Envelope Synthesis via Angelic Refinements. *Aditi Kabra*, Jonathan Laurent, Stefan Mitsch, André Platzer. TACAS 2024.
- Verified Train Controllers for the Federal Railroad Administration Model: Balancing Competing Brake and Track Forces. *Aditi Kabra*, Stefan Mitsch, André Platzer. EMSOFT 2022. *Best Paper finalist.*
- Geometry Types for Graphics Programming. Dietrich Geisler, Irene Yoon, *Aditi Kabra*, Horace He, Yinnon Sanders, Adrian Sampson. OOPSLA 2020.
- Online Verification of Commutativity. *Aditi Kabra*, Dietrich Geisler, Adrian Sampson. TAPAS 2020.

Teaching

Teaching Assistant, Carnegie Mellon University, Pittsburgh, PA

Software Foundations of Security and Privacy. *Fall 2022.*
Logical Foundations of Cyber Physical Systems. *Fall 2021.*

Teaching Assistant, Cornell University, Ithaca, NY

Text Mining for History and Literature. *Fall 2019.*
Introduction to Algorithms. *Spring 2018, Spring 2019.*
Data Structures and Object Oriented Programming. *Spring 2017, Fall 2017.*

Service

- Reviewing
  - Subreviewed for HSCC 2024.

  - Member of artifact evaluation committee, HSCC 2023.
  - Subreviewed for LICS 2023.
  - Subreviewed for NFM 2023.
  - Member of artifact evaluation committee, ASPLOS 2023.
  - Subreviewed for FM 2022.
  - Subreviewed for ICCPS 2022.
  - Subreviewed for iFM 2022.
  - Member of artifact evaluation committee, ASPLOS 2021.
  - Subreviewed for ICCPS 2021.

- Organized CMU programming languages area lunch talk series (PLunch) during the 2022-2023 academic year.
- Served as CMU Computer Science Department Student Ombudsperson in Spring 2023, Fall 2023 and Spring 2024.
- Started and ran formal methods reading group at CMU during the 2022-2023 academic year.
- Mentored students through software engineering summer internship projects at CodeDay Labs in summers of 2020 to 2023.

Other Research Experience

- Undergraduate researcher at Adrian Sampson's Capra research group at Cornell University. Contributed to Gator, a DSL for geometry types. *2018 – 2020.*
- Undergraduate researcher at Peter McMahon's quantum computing research group, the McMahon Lab, at Cornell University. Worked on understanding the scope and applications of Gaussian Boson Sampling. *2019.*

Awards

- Swartz Innovation Commercialization Fellow, 2023.
- Scholarship to attend Grace Hopper Conference, 2022.
- Promising Scholar, Maheshwari Vidya Pracharak Mandal, 2022.
- Scholarship to attend Women in Logic workshop at LICS 2021.

Software Engineering

Software Engineer (IC 2), Microsoft, Redmond, WA

Azure Reserved Instance Team. *January 2020 – August 2020.*

Software Engineering Intern, Microsoft, Redmond, WA

Azure Reserved Instances team. *May 2019 – August 2019, May 2018 – August 2018.*

Engineering Practicum Intern, Google, Mountain View, CA

Chrome User Metrics Analysis Team. *May 2017 – August 2017.*