CPS: Frontier: Collaborative Research: Correct-by-Design Control Software Synthesis for Highly Dynamic Systems

Jessy Grizzle, Aaron Ames, Hartmut Geyer, Huei Peng, and Paulo Tabuada

This project addresses highly dynamic Cyber-Physical Systems (CPSs) understood as systems where a computing delay of a few milliseconds or an incorrectly computed response to a disturbance can lead to catastrophic consequences. Such is the case of advanced safety systems on passenger cars, unmanned air vehicles performing critical maneuvers such as landing, or disaster and rescue response bipedal robots rushing through the rubble to collect information or save human lives. The preceding examples of highly dynamic CPSs all currently share a common element: their design is only made possible by a team of superb engineers with extensive experience in the design of similar systems and by laborious testing and fine tuning of parameters. A slight change in one of the software modules requires extensive re-testing of the overall system because the current understanding of these CPSs is insufficient to predict how changes in a module propagate through the overall system. We have seen this first hand in our experiments on MABEL, a bipedal robot at Michigan, where software for individual motion primitives performed as designed, but their handcrafted compositions had unpredictable behavior. This project will develop a formal framework for correct-by-construction control software synthesis for highly dynamic CPSs with broad applications to *automotive safety systems, prostheses, exoskeletons, aerospace systems, manufacturing, and legged robotics* . It addresses the target areas of *Science of CPSs* and *Engineering of CPSs* by:

(a) Formally designing low-level control software for highly dynamic CPSs through hybrid zero dynamics coupled with correct-by-construction software synthesis;
(b) Creating abstractions of such software modules with formal correctness guarantees;
(c) Automatically composing these abstractions to meet high-level specifications;
(d) Automatically refining the resulting abstract software descriptions to executable code while preserving correctness guarantees;
(e) Developing formal software synthesis tools applicable to a wide variety of CPS platforms;
(f) Applying the developed synthesis methodology to the domain of automotive safety systems, which provides a very concrete example of a highly dynamic CPS.

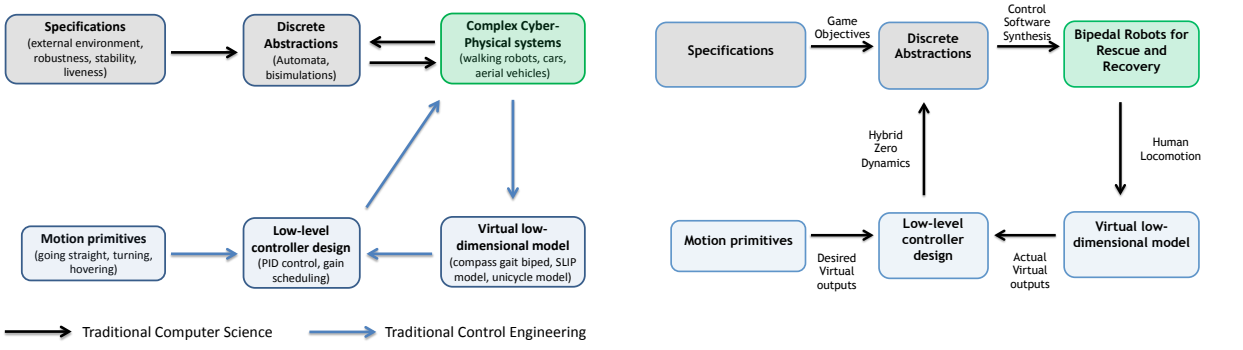

Figure 1: (a) Control software synthesis for complex cyber-physical systems, showing the traditional roles of computer science and engineering. (b) Control software synthesis applied to robotic walking, showing the connection between the "cyber" and the "physical" along with the specific tasks to be performed.