## Methods and Materials

To complete the proof for the drone braking system in Example 1, the specification consisting of constants, changing variables, assumptions, and the hybrid system must first be created.

In this case, the only constant variables, although arbitrarily constant, are and , which represent the location of the buffer line and the location of the wall the drone is approaching, respectively.

The changing variable are , the velocity, , the position of the drone, , the acceleration, and , a variable that is used in the reversionary controller to store the initial velocity of the drone after it passes the buffer.

The assumptions to be made prior to the establishment of the hybrid system are as follows: , meaning the drone starts at or before the buffer, , meaning the buffer zone, or the distance between the buffer and the wall, is nonzero, , meaning the drone is accelerating towards the wall when the program starts, and , meaning the drone is moving forward towards the wall when the program starts.

Finally, the hybrid system contains an that represents non-deterministic choice with two different dynamics on either side of the . The first describes the initial state of the system by simply declaring that and , with a domain restriction specified as . This ensures the advanced controlled only is allowed to start when the drone has not yet reached the buffer zone. The second side of the describes the dynamics of the reversionary controller. Within this side of the , a sequence of two steps is performed. First, with the expression , the velocity of the drone is recorded once the drone reaches the buffer. This velocity, , is needed to calculate important expressions used later in the proof. Second, the expression x'=v, v'=-(vi^2)/(2\*(E-bf)) & x>=bf sets , or the acceleration of the drone, to the expression . This expression was derived from the basic kinematic equations of motion using the initial velocity that was previously recorded and the distance between the buffer and the wall. The expression will make the drone decelerate towards the wall and have a velocity of zero once the drone reaches it. The domain restriction of these dynamics, , ensures that the reversionary controller is only allowed to start when the drone has passed the buffer. Lastly, the entire hybrid system is enclosed in a , which represents arbitrary repetition. This ensures the system can be repeated as many times as needed.

Finally, the postconditions of the proof are described: that , or the drone has reached the wall, and , or the drone has stopped. Since the system is surrounded with , it is established that the postconditions will use the existential quantified. In other words, this means the proof aims to show that these characteristics are true for *some* run of the system, as opposed to *all* runs of the system.

The proof of this specification relies heavily on the weakness of non-deterministic repetition when used alongside the existential quantifier. This allows the first steps of this proof to be simply using the iterated() tactic to separate the first three runs of the program from the repetition. After separating each iteration with the diamondOr() tactic and eventually removing the loop itself from the proof with the orR() tactic, we can isolate only the iterations of the loop that are needed to fulfill the postconditions. After this, the solve() tactic is used to solve and introduce a time variable to the differential equations of the hybrid system, and the existsR() tactic is used to specify the exact time at which the postconditions are true relative to all other arbitrary characteristics of the system. Finally, two branches are created that each require basic simplification using assumptions made earlier on in the proof, and the proof can be completed with quantified elimination. In other words, KeYmaera’s can complete the proof because the final expressions are trivially true.

The increased complexity of the proof for Example 2 has slowed progress and not allowed a full specification to be written. However, some progress has been made in determining the conditions for the start of the reversionary controller. This work must be expanded upon for a full specification to be written and subsequently proven.