CS 580 Specification of Software Systems

Homework 06: Electronic brake safety.

Your company accepted a contract to develop the software for an electronic emergency/parking brake to be used in a luxury line of cars. The emergency braking system employs two dedicated microprocessors to ensure full redundancy and rapid response. The driver presses and releases a colorful button to control the emergency brake; the result may be full engagement or disengagement of the emergency brake involving all four wheels or merely the smart application of additional braking power under certain conditions.

The first step in developing the electronic brake software is to specify the requirements for the entire system. Actually, the contract requires for the software to be provable correct. As such, you are asked to develop a formal specification of the electronic brake system keeping in mind usability and the safety of the driver.

Here are some useful hints for you to consider:

1. Start with a description of the abstract state the system including the events (press and release the button) and data (state of the brake and of the vehicle motion) needed to make correct decisions about applying the emergency brake.
2. Invariants can be used to specify integrity constraints; unless relations can be employed to constrain state transitions; and leads to properties can be used to define progress obligations.
3. Keep the specification simple, e.g., avoid relying on continuous variables. Working with a concept such as “high speed” is easier to manage than considering the exact speed of the vehicle.