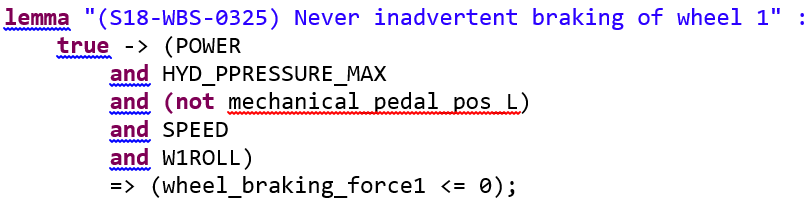
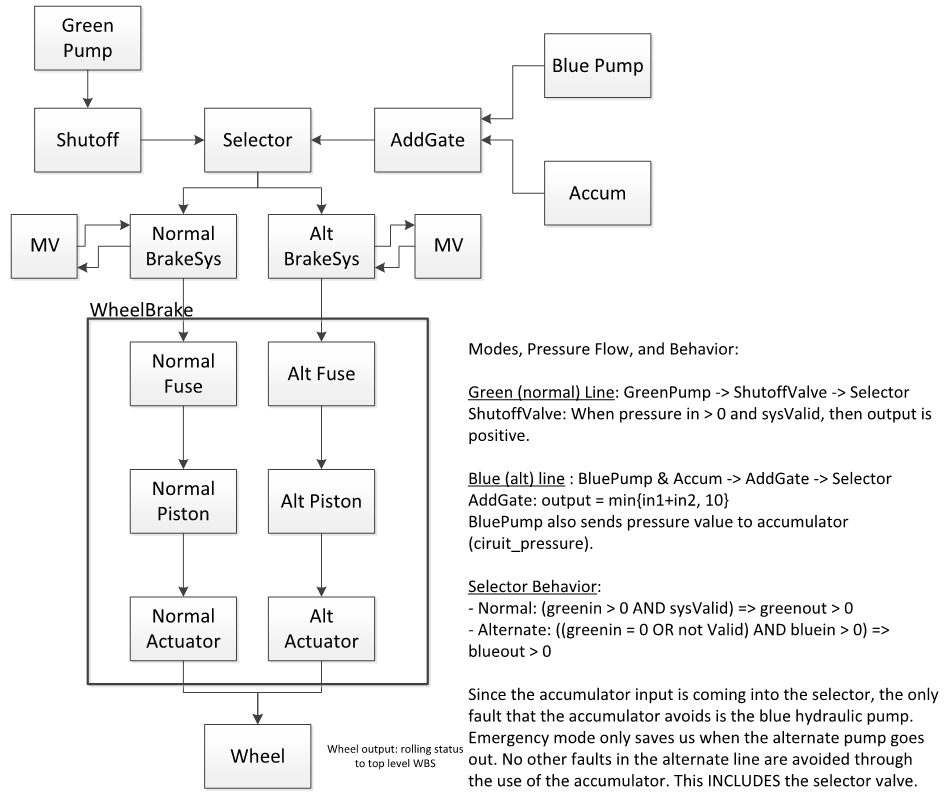
The requirement of interest is never inadvertent braking. Since we have looked at this in the past, I decided to stick with it for now. We can of course change if we want. 

1. The Sensor: The simplest thing we could do that directly influences this lemma is the sensor component. We have used it previously in other examples and it is the more straightforward of subcomponent issues to address. If there is no command in normal mode for brakes, the sensor states that there is a command, and braking is commanded. The possible fix is redundancy in the sensors, implement some kind of monitor to determine which sensor information to use, and that is pretty much it. Simple to understand and not very complex to mitigate.

The other examples will need a bit of a description of the physical system. It’s good for everyone to read through this and understand it anyways.

Here are notes and a diagram of the physical system so you can see the flow of things and where the subcomponents are sitting in reference to the whole model.



Note: The accumulator was in a different location early on in the AIR6110 document (beneath the selector valve) but was moved because there are cases in which during normal mode, the accumulator could supply pressure. They moved it to mitigate this problem and thus emergency mode only kicks in when blue pump goes out (AIR6110 pg 67 and fig 40).

Notes on some contracts and info about the physical system that I wrote up a while ago:

*Modes, Pressure Flow, and Behavior:*

Green (normal) Line: GreenPump -> ShutoffValve -> Selector

ShutoffValve: When pressure in > 0 and sysValid, then output is positive.

Blue (alt) line : BluePump & Accum -> AddGate -> Selector

AddGate: output = min{in1+in2, 10}

BluePump also sends pressure value to accumulator (ciruit\_pressure).

Selector Behavior:

- Normal: (greenin > 0 AND sysValid) => greenout > 0

- Alternate: ((greenin = 0 OR not Valid) AND bluein > 0) => blueout > 0

Since the accumulator input is coming into the selector, the only fault that the accumulator avoids is the blue hydraulic pump. Emergency mode only saves us when the alternate pump goes out. No other faults in the alternate line are avoided through the use of the accumulator. This INCLUDES the selector valve.

Questions about subcomponent behavior:

- When does the accumulator output pressure?

o Output is positive if and only if blue pump output is zero.

- When is blue output zero?

o Output is zero if we have no power or the top level supply is zero.

- Is the top level supply ever zero?

o It could be. The assumption binds it between 0 and 10 inclusive.

- Accumulator can kick in when exactly?

o Case 1: Top level supply for blue pump is zero.

o Case 2: We have no power to the pump.

o Case 3: A fault is active on the pump which causes output to be zero.

- When is the green line used?

o When we have power to the green pump, when the “system is valid”, and when the top level green supply is positive.

- What causes green line to go bad (i.e. what activates blue line)?

o Case 1: No power to green pump

o Case 2: Top level green supply is zero

o Case 3: System is invalid

o Case 4: Fault on green pump causes output to be zero

o Case 5: Fault on ShutoffValve causes its output to be zero

- If we have all cases covered from previous question and wheel does not receive pressure (normal line), does the system switch to alternate mode?

o No, there are no flags or commands to Selector, Pumps, or Accumulator regarding pressure at the wheel and there is no delay in feedback regarding pressure at the wheel.

In this setup of the system, the Alternate mode only protects against faults that occur in the GreenPump or ShutoffValve. The Emergency mode only protects against a fault in the BluePump.

The Alternate mode does kick in when the BSCU is invalid and requires mechanical braking, thus eliminating the need for electrical components when something goes wrong in the digital side of the system.

**Possible subcomponents:**

(2) Selector Valve: Stuck at previous value (for both alternate and normal modes). Previously braking was commanded, now its not, output reflects previous state and pressure is supplied.

(3) Accumulator: Stuck open.

(4) MeterValve: Stuck open.