Validation SLR

The high level specification defines the basic flow of the use-cases, user constraints and safety properties. At the same time, we validate the System Level Requirements through the high level specification. “Sort unsorted discs” is correct, because the high level specification mentions that the machine should sort discs. Aborting the process happens because in every machine something could go wrong and thus it needs to be able to be stopped at any point in time. “Starting the machine” and “Stopping the machine” are actions which also is needed for machines because else you couldn’t make them stop or start doing what they are supposed to do. “Booting up the machine” and “shutting down the machine” is required, because the disc sorter has to be turned on and off, in order for it to fulfil its purpose.

Before the start buttons is pressed the user is required to place all discs to be sorted in the container unit. The discs should be placed in the container, so that the machine is able to sort the discs.  
While the machine is running the user is not allowed to move the machine or touch anything except the buttons. If the user makes contact with either the conveyor belt or the discs while they’re on the conveyor belt, the machine might not be able to separate the discs correctly.  
When the abort button is pressed or the machine has to be shut down, the user is required to remove all discs that are neither in the container unit nor sorted. The user is supposed to do this, so that the machine will be able to restart the sorting process with a new disc.

After pressing an emergency button, within 50 ms there should be no moving parts in the machine. The machine should immediately abort its current process, according to the high level specification, although this is not realisable. Therefore, this is set to be within 50 ms.

According to the High level Specification the machine should stop sorting if there is no more disk signaled after 4s. We made this into a safety property, because a running machine with no use is only going to possibly harm people getting in contact or the machine itself.

According to what the high level specification offer, there is nothing that could stop the assembly program as long as the code is correctly written for this purpose, we don’t consider accidents and flaws, the only way for the program to end is by powering off the machine.

The outputs connected to the h-bridge may never be powered on at the same time. If this happens, the PP2 processor short circuit, and the machine won’t work anymore.