

# Risk Assessment for the Train Module of the Port Authority of Allegheny County Transit Control System

Nathan Altay Hunter  
Software Engineer  
Bazinga! Industries

There are three categories of risks involved in this project. The level of risk is determined by its consequences; low risks are unlikely to cause any significant problems, while high risks are likely to create issues.

Low Risk

* Train controller instructs incorrect light state

Due to a miscommunication between the train controller and the train, the train could receive the incorrect light state and turn the lights on when they should be off, or vice versa. This may inconvenience passengers but should not have any serious consequences.

.

Medium Risk

* Train controller instructs incorrect door state

A miscommunication between the train controller and the train could cause the train to incorrectly open the doors. Although this is unlikely to have negative consequences it could cause injury or fatality if a passenger is leaning against a door.

* Acceleration is incorrectly calculated

Due to defects in the code the train could potentially miscalculate the acceleration necessary to reach its target speed. It may accelerate at unsafe rates potentially damaging the engine.

* Running out of time on project

This System is very complex and leaves room for failure due to time constraints Failure is always and option…..

High Risk

* Train is created with incorrect preset values

When the train is added to a track it must be given several preset values. These include its physical speed and acceleration limits, its mass, and its dimensions. If these are incorrect they could cause the train to accelerate at incorrect rates or attempt to fit through tunnels which are too small for it.

* Communication with train controller is broken

The train may lose all communication with the train controller. This is an incredibly dangerous scenario. The train no longer has any instructions and the only safe course of action is to stop the train.

* Train has a break failure

A break failure is the most serious problem possible. Unlike every other scenario the train cannot deal with a break failure by stopping the train; all that can be done is to prevent the train from accelerating and wait for friction to bring the train to a gradual stop.

* I do not currently know C#

I must learn C# in order to implement the Track Model. This is a high risk as a new language can cause learning curve.

* The Train Module will not properly interface with the other System Modules

The system may not function at all if one module will not properly interface.

* Not fully understanding the operation of a train control system

This could cause overlapping function between modules that could make interfacing them difficult

* Not catching a bug until final release (High for non simulation)

The final product could contain a bug that may cause unsafe failure conditions