Invariants

✓ If train is present then alarm is active & barrier is down.

✓ If no train present then alarm inactive & barrier is up

✓ If error/default, barrier should be down

✓ If multiple trains in area keep barrier down

Assume that a single train will never cross both sensors

Trains travel fast enough to leave critical area after triggering departure sensor

If main power loss, we have enough backup power to at least close barriers

✓ The approach & depart sensors will never detect the same train. For short their seperation will be greater than length of train

The trains will always take at least 10 seconds before reaching critical section