**Railway Exercise**

**System Requirements**

We consider the formal specification of a railway system using the Event-B language. The rail network is divided into track sections. There may be many trains operating on the rail network but at most one train can occupy any one section. Trains may be moving or stopped. A single train may occupy several sections. In particular, while a train is moving from one section to another it will occupy both sections simultaneously. A train acquires occupancy of a track section when part of the train enters that section; it releases its occupancy of a track section when the last part of the train leaves that section.

Some of the sections will represent platforms where trains can stop. For safety reasons, a train’s doors may only be open if a train is stopped at a platform. A platform consists of a single section.

**Tasks**

1. Produce an Event-B model of this system using the following steps:
   1. Produce a numbered list of informally described requirements from the above description, to help in your modelling.
   2. Create a class diagram for the system showing the required sets and relationships between sets. This will help you specify appropriate Event-B sets, etc. You do *not* need to consider the adjacency of track sections in your modelling.
   3. Specify an Event-B context with appropriate types, constants and their properties.
   4. Specify machine variables and invariants that model the dynamic behaviour of the system, and its constraints. The variables should capture the relationships between trains, sections and platforms. The variables should also model the status of train doors and whether each train is moving or not. Ensure that the safety requirements on the doors are modelled in the invariants.
   5. Specify an event to open the doors of a train and an event to start a train moving.
   6. Specify an event to model a train taking occupancy of a track section and an event to model a train releasing its occupancy of a track section.
   7. List any ambiguities you uncovered in the system requirements and how you addressed them.
   8. For each of the constraints in (a), justify informally how it is modelled in your Event-B model.
2. After some high-level safety analysis it was decided that there should be an emergency override on the doors so that they can be opened on any section (not just a platform) whenever an emergency arises provided the train is stopped. The driver is expected to stop the train when an emergency arises. The emergency status of the train can be activated by the driver or the guard using special key-controlled switches located in each carriage and in the driver’s cab.
   1. Construct a new version of your Event-B model, taking account of the emergency door override feature outlined above.
3. Explain how your Event-B model could be extended to incorporate adjacency of sections, i.e., which sections immediately precede or follow which other sections. How would you express the fact that a train should only occupy a set of adjacent sections?