

# The Metro Refinement Example

Andy Edmunds

University of Southampton

February 6, 2013

# The Metro System

- ▶ Import the exercise model from `MetroSafety_Exercise.zip`
- ▶ Read and understand, as much as possible, the variables, and events.
- ▶ Do not focus, to much, on the axioms, and invariants at this stage; but the following may be useful.
  - ▶  $CDV$  is a (carrier) set of track sections.
  - ▶  $cdvrel = CDV \leftrightarrow CDV$
  - ▶  $cdvfn = CDV \rightarrow CDV$
  - ▶  $tcl \in cdvrel \rightarrow cdvrel$  is the transitive closure of track sections.
- ▶ Add a message send event, indicating that a train may proceed to its next section. Introduce  $tmsgs \in trns \rightarrow \mathbb{P}(\text{BOOL})$
- ▶ Model receipt of the permission by introducing an event, and  $permit \in trns \rightarrow \text{BOOL}$
- ▶ Modify *enterCDV*, *leaveCDV*, *brake* (when a train's permit is false), and *addTrain*.