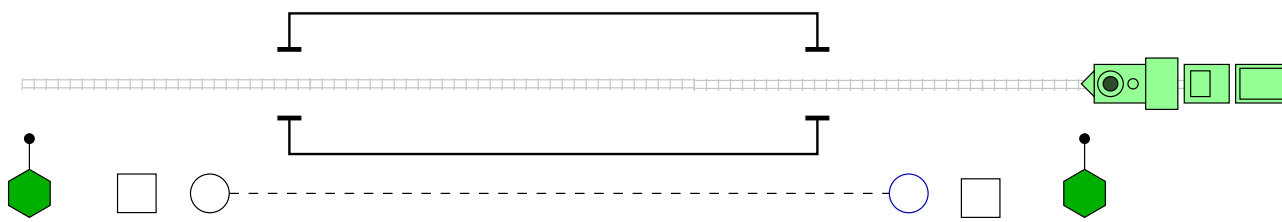
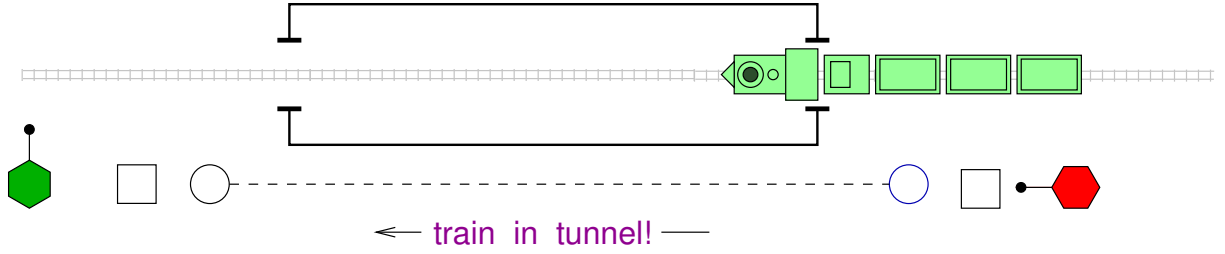
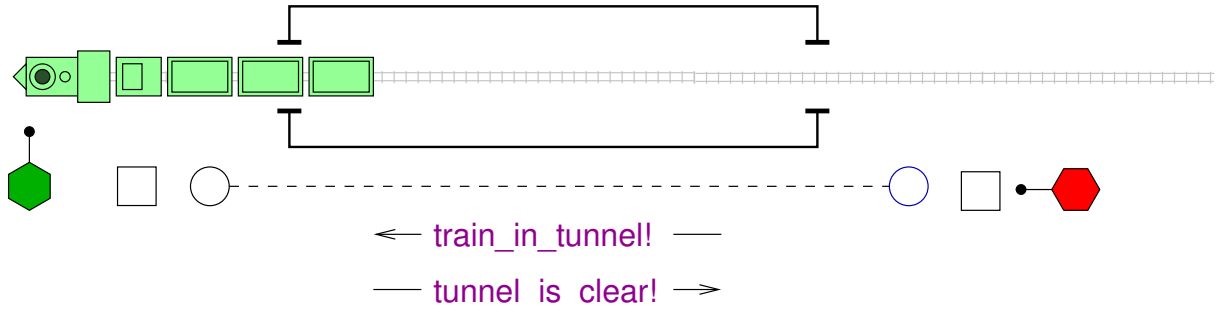


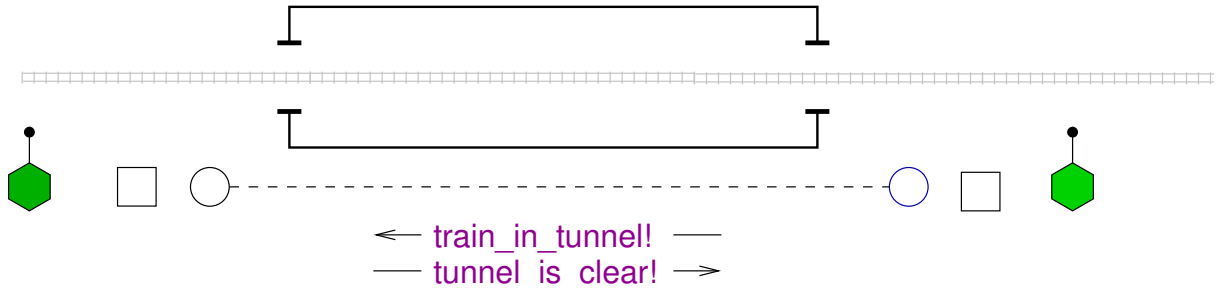
INVARIANT: "There is never more than one train in the tunnel at a time"

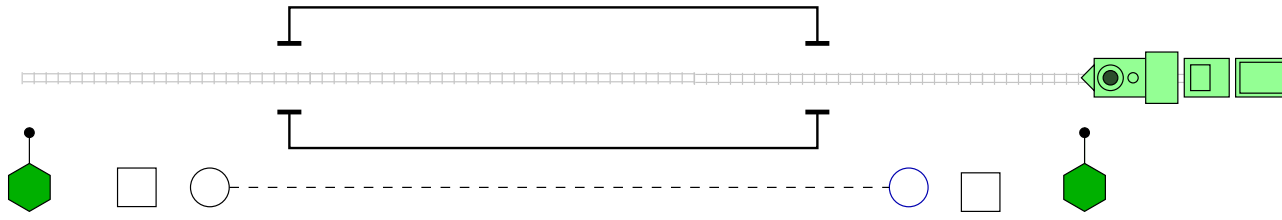


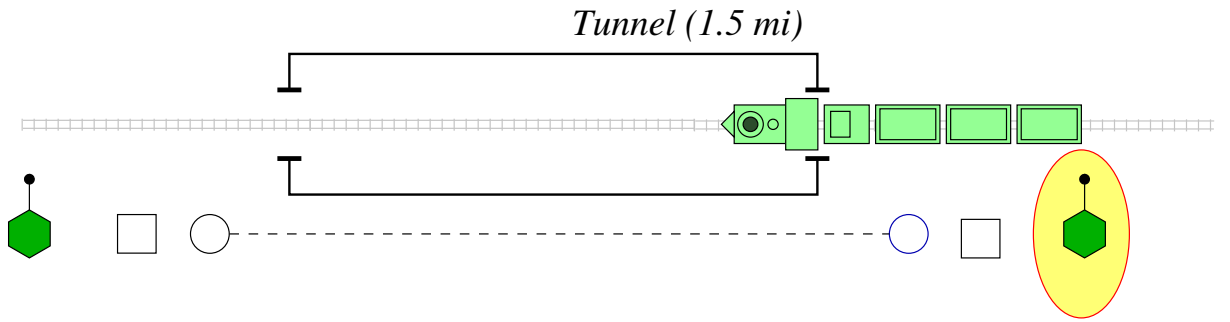


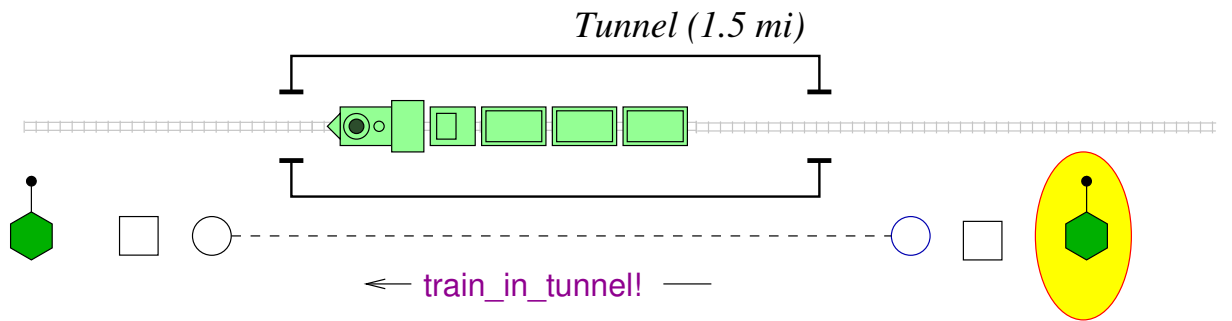
← train in tunnel! —

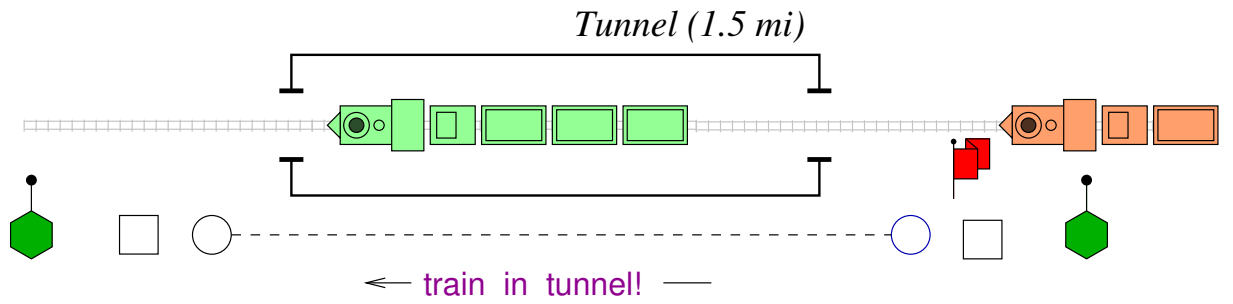


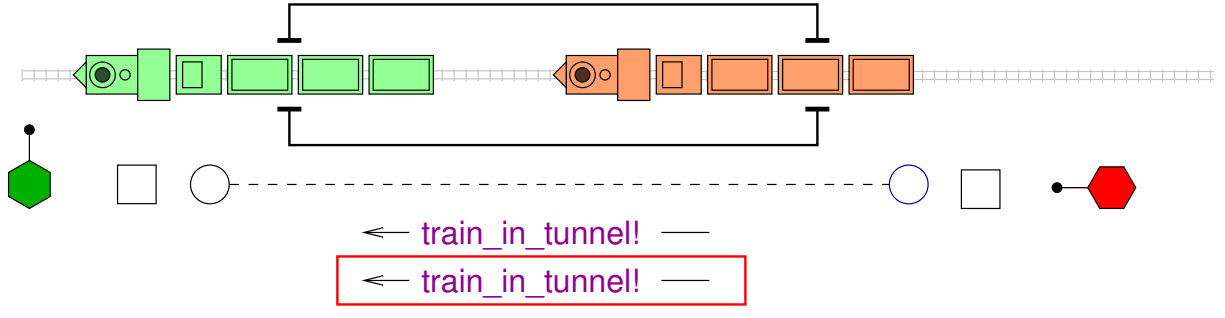


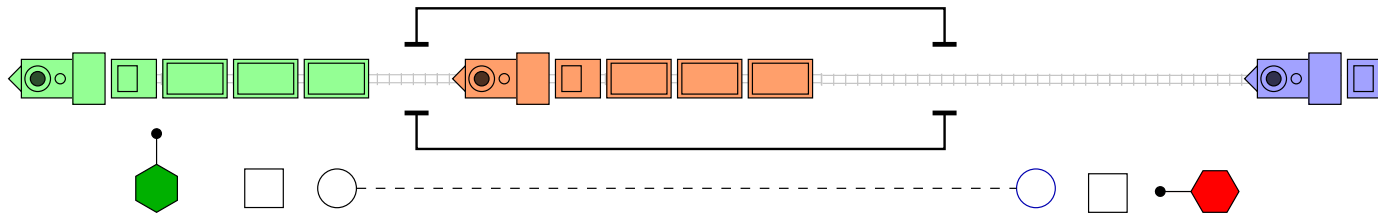




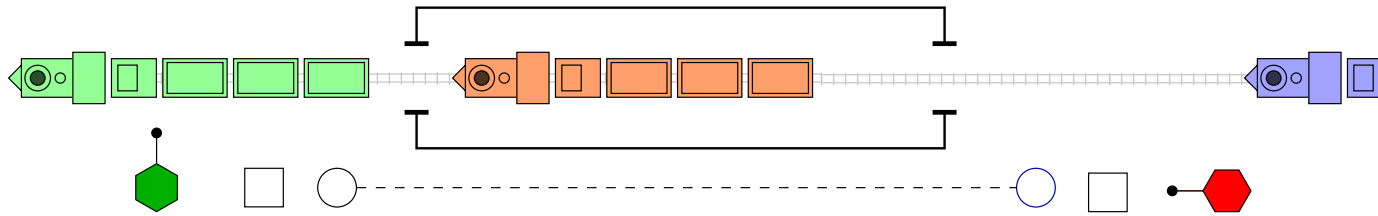




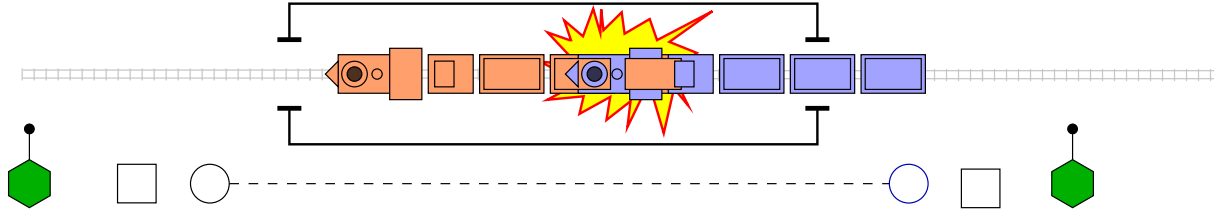




← train_in_tunnel! —
← train_in_tunnel! —
← train_in_tunnel? —
— tunnel is clear! →



← train_in_tunnel! —
 ← train_in_tunnel! —
 ← train_in_tunnel? —
 — tunnel_is_clear! →
 ← train_in_tunnel? —
 — tunnel is clear! →



← train_in_tunnel! —

← train_in_tunnel! —

← train_in_tunnel? —

— tunnel_is_clear! —>

← train_in_tunnel? —

— tunnel is clear! —>

- Most system failures are due to *unanticipated scenarios*
 - Failure of *component* (fault tolerance)
 - Unexpected sequence of events
 - etc.*
- Failures occur *at interfaces*
- Inconsistent interpretations at different observation points