The *Railway Disaster* Exercises

The idea is to analyse the events leading up to historic railway disasters with the principles of LSD specification in mind. This analysis will illustrate the subtlety of the relationship between perceptions and privileges of agents and their corporate behaviour.

Note that it isn't difficult to write a program to simulate any of these accidents in a superficial sense ... what would be very difficult (if even possible) in general would be to simulate them in such a way that we could interrogate the simulation for info about the perception of the agents at an intermediate stage.

The basic idea of observations of agents, perceptions and actions are clear. We've seen how definitions can express *interpretation of observation* (cf the guard) that can be deemed "knowledge".

These examples illustrate practical difficulties that beset LSD specification in general interaction between agents (i.e. agent-oriented analysis).

Issues include:

How oracles, handles and privileges of agents are influenced by

locality - how are the agents distributed
roles - the same agent may play different roles
authority - one agent may delegate to another
knowledge
- motivations for action, cultural context, acquired experience, skills

How the effect of actions is influenced by

commitment - when is an agent required to act, pledged to act
conflict - two agents can act at cross purposes
synchronisation - when must actions occur at the same time
environment
- how do environmental factors influence outcome of actions
modes of communication - e.g. intermittent vs persistent

What can be modelled in LSD?

There's a spectrum from routine programming as interaction between reliable agents to very complex subjective human interaction in which emotion, judgement and intelligence etc play a part. Where does LSD fit into this? where is it inappropriate? are there criteria for its application to particular situations?

What can we identify as making safe automatic train control possible?

Consider for instance

making communication concrete through some physical ritual

using automatic equipment to advise the human agent

using automatic equipment to coerce the human agent

The place of **safety** and **liveness**. [Informally, safety guarantees that, provided protocols are followed, whatever happens isn't dangerous, and liveness guarantees that progress can be made towards a goal.]

One motivation for these exercise is that – presumably – activity that we can formulate more effectively in LSD will also be easier to automate.

Reference

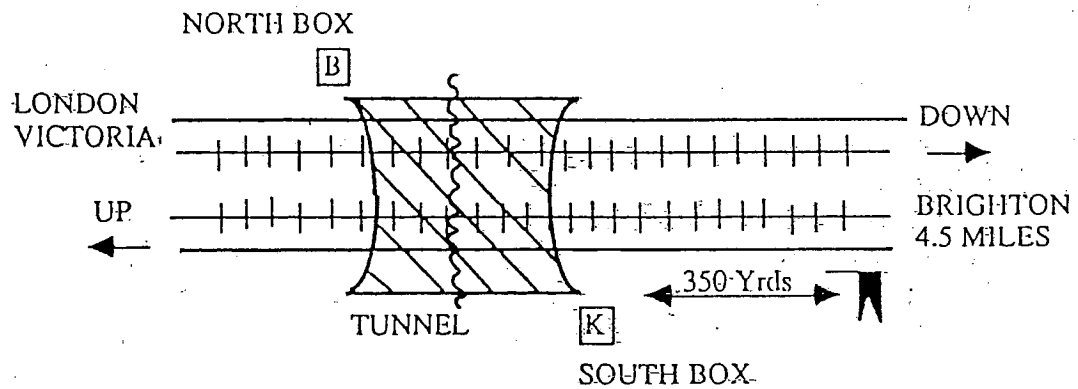
L.T.C. Rolt *Red for Danger*, The Bodley Head Press 1955

Historic Railway Accidents 1

Clayton Tunnel **August 25th 1861**

Three heavy trains leave Brighton for London Victoria on a fine Sunday morning, travelling on the London, Brighton and South Coast railway. The time interval system is applied along the track, except for the Clayton Tunnel – the first railway tunnel to be protected by a telegraph protocol designed to prevent two trains being in the tunnel at the same time

The layout at the Clayton Tunnel is as in this figure:



There is a signal box at each end of the tunnel. The North Box is operated by **B**rown and the South by **K**illick. K has been working for 24 hours continuously. In his cabin, he has

a clock
an alarm bell
a single needle telegraph

and a handwheel with which to operate a signal 350 yards down the line. He also has red (stop) and white (go) flags for use in emergency.

The telegraph has a dial with three indications thus:

NEUTRAL

OCCUPIED CLEAR

When K sends a train into the tunnel, he sends an OCCUPIED signal to B. Before he sends another train, he sends an IS LINE CLEAR? request to B, to which B can respond CLEAR when the next train has emerged from the North end of the tunnel. The dial at K's end only displays OCCUPIED or CLEAR when the appropriate key is being pressed by B – it otherwise displays NEUTRAL.

The distant signal is designed to operate automatically so that it returns to danger as a train passes it, but if this automatic mechanism fails, it rings

the alarm in K's cabin. This signal is to be interpreted by a train driver either as *all clear* or as *proceed with caution*.

The three trains leave Brighton according to the following schedule:

		Times of departure		
Train (from)	Size	As advertised	Stationmaster	**Actual**
1 PORTSMOUTH	16	8.5	8.22	**8.28**
2 BRIGHTON EX	17	8.15	8.27	**8.31**
3 BRIGHTON ORD	12	8.30	8.36	**8.35**

where the actual times of departure, as established at the inquiry, differ from those alleged by the stationmaster. (Officially there must be a time interval of at least 5 minutes between trains.)

The accident

When train 1 passed K and entered the tunnel the automatic signal failed to work. The alarm rang in K's cabin. K first sent an OCCUPIED message to B, but then found that train 2 had passed the defective signal before he managed to reset it. K picked up the red flag and displayed it to Scott, the driver of train 2, just as his engine was entering the tunnel. He again sent an OCCUPIED signal to B.

K didn't know whether train 1 was still in the tunnel. Nor did he know whether S had seen his red flag. He sent an IS LINE CLEAR signal to B. At that moment, B saw train 1 emerge from the tunnel, and responded CLEAR. Train 3 was now proceeding with caution towards the tunnel, and K signalled *all clear* to the driver with his white flag.

But S had seen the red flag. He stopped in the tunnel and cautiously reversed his train to find out what was wrong from K.

Train 3 ran into the rear of Train 2 after travelling 250 yards into the tunnel, propelling Train 2 forwards for 50 yards. The chimney of the engine of Train 3 hit the roof of the tunnel 24 feet above. In all 23 passengers were killed and 176 were seriously injured.

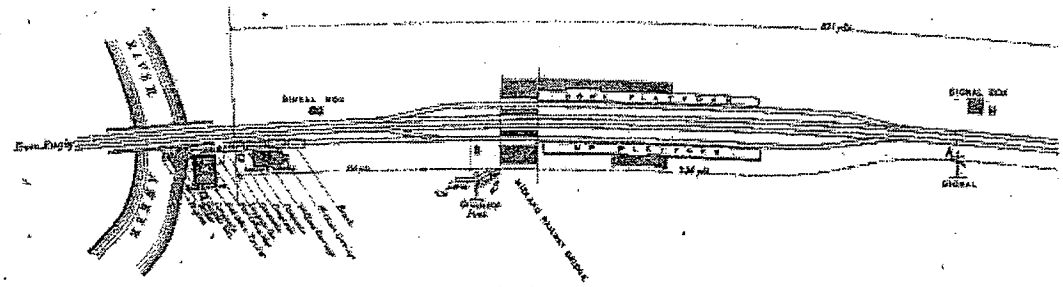
Your agenda:

a. analyse the perceptions and privileges of the agents involved
b. discuss the role of knowledge (interpreted perception) in the events
c. what relevance has the mode of operation of the telegraph?
d. what is the role of the automatic signal device?
e. to what extent is time an important factor in the accident

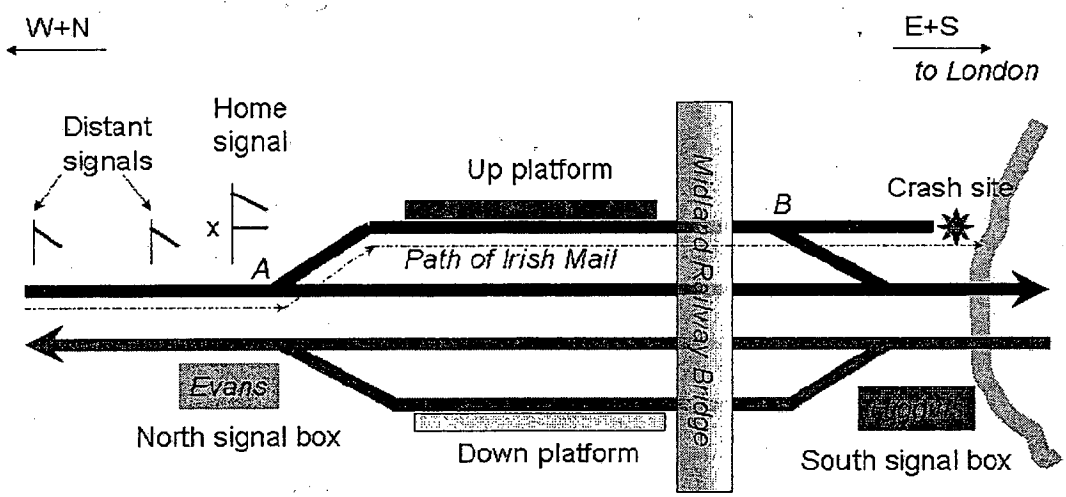
What recommendations would you make for avoiding a recurrence?
What agents do you consider primarily responsible for the accident?
Is it possible / appropriate to write an LSD specification for the agents?
If so, what insight can be gained from this?

Tamworth **September 4th 1870**

The station layout at Tamworth in 1870 was shown in the Board of Trade report thus:



For the purposes of explaining the circumstances of the accident, the following diagrammatic representation may be more helpful. It involves a reorientation that brings the location of key features into line with a modern map of Tamworth. The station itself is oriented from west to east, with track turning away to the north to the west and to the south in the east.



The speculative account of the accident that occurred on September 4th 1870 that follows is based on trying to read between the lines of the Board of Trade report, in which some prerequisite knowledge of the technologies of the time is implicit. It is not always entirely clear whether my interpretation of the situation and practices is correct – something that might be itself a motivation for developing an EM construal. I have also simplified the terminology – e.g. the report refers to distant, intermediate and home signals, but the intermediate signal is here being classified as distant.

The station catered for express trains (or more generally "through trains") that didn't stop, but the points could also be set so that trains stopped at the platforms. Through trains passed through the station on the up and down main lines, and stopping trains visited the up and down platform lines. The points at the North (respectively South) end of the platform were controlled from the North (respectively South) signal box. The points at the South were interlocked so that when the points on the main line were set for a through train the points on the platform line (at B) were automatically set for

the siding that led to a dead end near the engine house (not depicted, but adjacent to the crash site in the diagram). This siding was only used exceptionally and in typical operation (as recommended in a memorandum issued on the 9th November 1869) the points would be set in such a way that a stopping train that overshot the platform would be directed back on to the main line.

Principles of interlocking were used in communicating information about the status of the points to train drivers (via signals). For instance, the mechanism of the home signal was such that (e.g.) the signal for the main line at A could only be lowered (to indicate that a train could pass through the station on the main line) if the points were first set to the main line. When the signal was then lowered, the points would be locked to the main line. Because of this locking, in order to reset the points at A, it was first necessary to set the corresponding signal to danger by raising it, then to adjust the points, and then to reset the signal.

There were two signal boxes at Tamworth station; on the day of the accident the South was being manned by Higgins and the North by Evans. H and E could not see each other because of the station buildings and the Midland railway bridge crossing above the line at right angles. A telegraph had just been installed but was not yet in operation, so that H and E still using the previous technology for communicating about approaching trains.

It would appear from the description in the Board of Trade report that communicating information about the status of the points from one signal box to the other made use of discs that were based on interlocking mechanism similar to those associated with signals. For instance, when the signalman at the South box had set the South points in readiness for a through train, he was then able to change the position of a disc in the North cabin by operating a lever. Whilst this disc remained in this position, it gave the signalman in the North box necessary information about the current status of the South points, together with the reassurance that the South points were then locked to the main line.

Discs were used in conjunction with a gong mechanism. The signalman at one signal box could pull a lever to sound a gong in the other. For instance, when the signalman at the North box wished to inform the signalman at the South box about the pending arrival of a through train (respectively stopping train) on the up line, they pulled the lever to ring the gong once (respectively twice). The train would then only be allowed to proceed (through appropriate setting of the signals) when the disc in the North cabin indicated that the South points had been appropriately set.

A train that approached the station on the up line (from the North) passed signals on three occasions, first at the distant signals, then at the pair of home signals indicated (see the diagram). Notice that only the home signals were interlocked with the points, so that it was possible (as in the diagram) for a through train to encounter distant signals set to clear even though the points were set for the platform line, and the home signal for the main line was accordingly set to danger (as marked with an 'x' in the diagram). The enquiry highlighted the absence of other interlocking mechanisms such as would have prevented the points at A and B being configured in what the accident revealed to be such a potentially dangerous state.

The accident

The accident occurred in the middle of the night. At 3.53 a.m., the signalling arrangements for the arrival of the next train were put in place. H in the South Box, was expecting the late running Irish Mail train. H set the South points to the main line to prepare for the Mail to pass through without stopping. Because his watch had stopped, E was confused about the train schedule, and expected a stopping goods train that would call at the up platform. E set the points at A for the loop line, so that the loop signal was set to clear and the main signal to danger on the home signal.

The Mail arrived at speed at 4.09 a.m., thirteen minutes late. It came in to the station at speed after passing the distant signals at clear, then rocked across the points at B, and thundered past the up platform. At this point, H might still have been able to redirect the Mail to the up main line by moving back the lever that operated the disc in the North box cabin and switching the points at B, but his view was obstructed at that moment by a goods train passing his box on the other line. In the event, the Mail crashed through the stop block at the end of the siding into the middle of the River Tame. The driver, fireman and one passenger were killed in the accident.

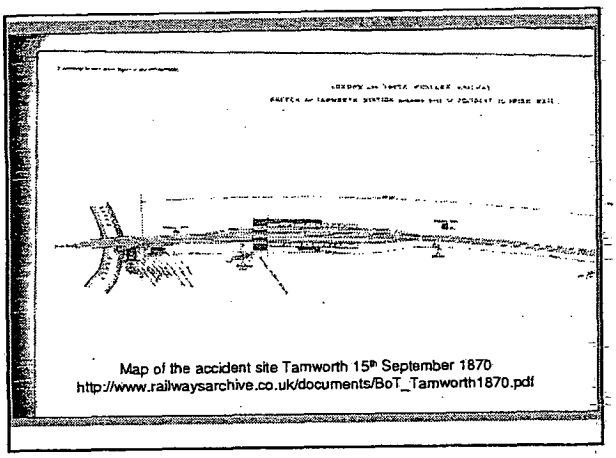
Some issues to reflect on:

a. analyse the perceptions and privileges of the agents
b. what role does time play in the accident?
c. where is knowledge (interpreted perception) involved?
d. what are the most significant environmental factors?
e. what interlocking would have helped?
f. had there been a telegraph, what communication was necessary?
g. what assumptions about scheduling could have guaranteed safety?
h. would you hold anyone responsible for the accident?

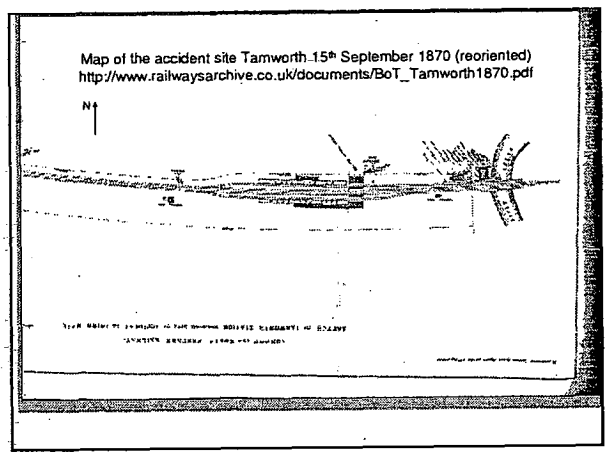
Can you devise an LSD account for the signalmen agents?
Can you model the interlocking arrangements as dependencies in EDEN?

References

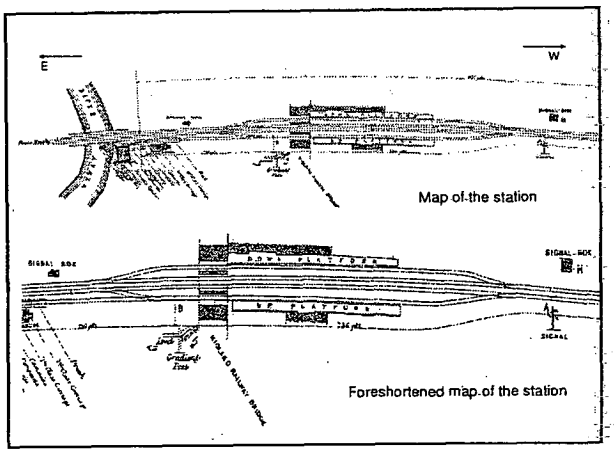
L.T.C. Rolt, *Red for Danger*
http://www.railwaysarchive.co.uk/documents/BoT_Tamworth1870.pdf



Map of the accident site Tamworth 15th September 1870
http://www.railwaysarchive.co.uk/documents/BoT_Tamworth1870.pdf

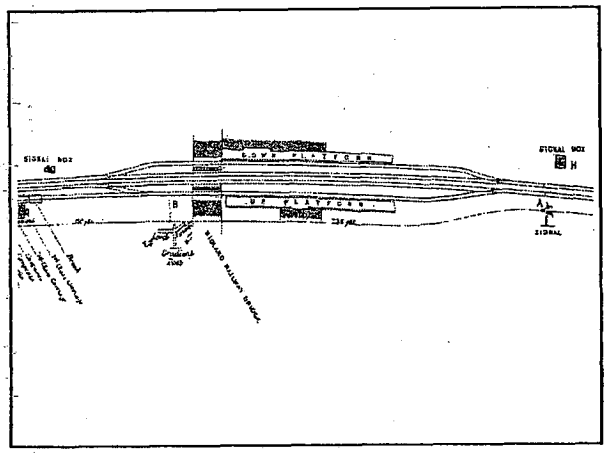


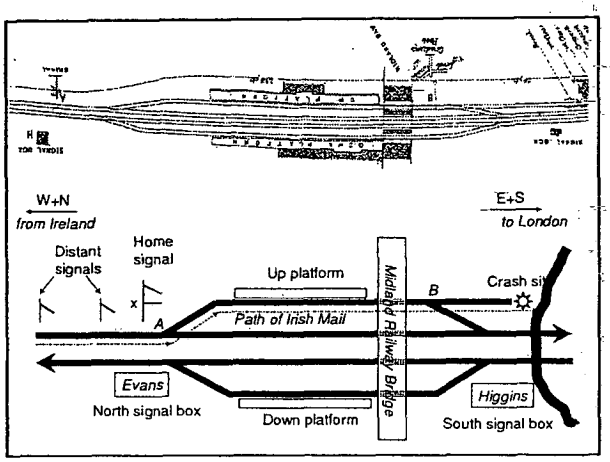
Map of the accident site Tamworth 15th September 1870 (reoriented)
http://www.railwaysarchive.co.uk/documents/BoT_Tamworth1870.pdf

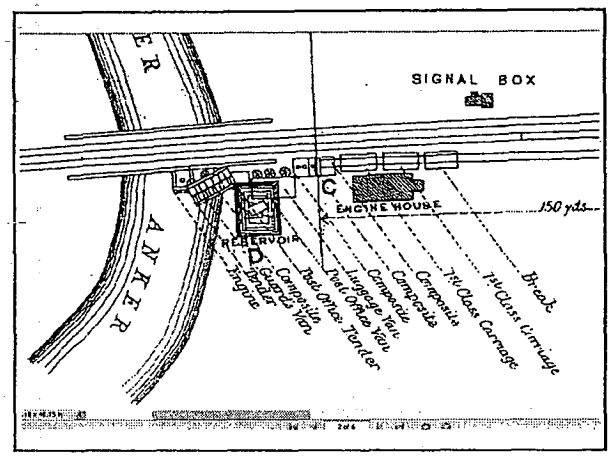


Map of the station

Foreshortened map of the station







Some notes on the Tamworth 1870 accident scenario

To appreciate the attached fragments of an LSD account, you need to have the picture of the accident scenario with signalmen E and H and points labelled A and B in mind. The 'driver' agent here is the driver of the Irish Mail train. (This is the artefact that, in conjunction with the referent - in your imagination! - informs the LSD account.) Note that there are many physical factors, relating to lengths of trains, location and distances between points, feasibility of observation of various kinds etc, about which the artefact gives useful insight but that are *not in* the LSD account. Some of this information is so obvious that we wouldn't dream of identifying it explicitly when we develop the account. For instance, the Irish mail train encounters the points at A before it reaches the points at B (isn't that obvious?) - and trains don't come up the river either (but even that could be different in some surreal computer game).

Standard protocols ("from training manual")

```
agent driver {
        oracle distantsignal
        handle speed_of_train
        protocol
                distant_signal==CAUTION --> speed_of_train = SLOW

}
```

.. this is OK if you don't consider brake failure or icy etc - otherwise:

```
agent driver {
        oracle distantsignal
        handle brakePos
        derivate speed_of_train = f(brakePos, ... )
                                  ## '...' on RHS for environmental factors
        protocol
                distant_signal==CAUTION --> brakePos = ON

}
```

A first approximation to the North signalman agent account is:

```
agent signalmanE {
        oracle next_train, homeUPsignal_status, homeMsignal_status, pointA_status
        derivate
                next_kind_of_train is typeof(next_train)
                status_or_next_train is                                    ;
                        f(next_kind_of_train, schedule)       // status is STOPPING or THROUGH
        handle homeMsignal_status, pointsA_status
        derivate homeUPsignal_status = if (homeMsignal_status = CLEAR) then DANGER else CLEAR;
        protocol
                (next_kind_of_train == STOPPING)
                        --> pointsA_status = TO_PLATFORM; homeMsignal_status = DANGER;
                (next_kind_of_train == THROUGH)
                        --> pointsA_status = TO_MAIN; homeMsignal_status = CLEAR;
                ....
}
```

Note that this doesn't permit both home signals to be set at DANGER. This is a serious flaw, not only because this is an essential state from the point of view of safety (imagine e.g. if the whole station were to be on fire), but also since both home signals at DANGER is a precondition for it to be possible to switch the points at A. This means that the derivate is really an unsatisfactory simplification: indeed, the positions of the home signals can *at any time* be set at DANGER.

A better account captures the idea that the signalman follows two different protocols to set up the points and signals for the arrival of stopping and through trains. Note that there is an invariant relationship (guaranteed by the interlocking mechanism) whereby `homeMsignal_status == CLEAR => pointsA_status == TO_MAIN`. (It is not mechanically possible to set the home mainline signal to clear unless the points at A are correctly set, and once the signal has been lowered, it is mechanically impossible to change the points at A.) On that basis, the privilege

```
(pointsA_status == TO_MAIN) and (homeMsignal_status = CLEAR) --> homeMsignal_status = DANGER
```

can be 'equivalently' expressed as:

```
(homeMsignal_status = CLEAR) --> homeMsignal_status = DANGER.
```

A similar observation applies to setting the home platform signal to danger ("the signalman can change a signal at CLEAR to DANGER at any time"). Notice here that in accepting that such relationships cannot be otherwise we are taking steps towards a view of the mechanical technology as 'completely reliable' that is part of the much larger move towards "taking mechanisms for granted" that is characteristic of classical computing. There is probably some justification for this, when we consider that, once the technology was mature, mechanical failure of interlocking mechanisms was much less likely than human error to be at the root of railway accidents.

```
agent signalmanE {
        oracle next_train, homeUPsignal_status, homeMsignal_status, pointA_status
        derivate
                next_kind_of_train is typeof(next_train)
                status_or_next_train is
                        f(next_kind_of_train, schedule)        // status is STOPPING or THROUGH
        handle homeMsignal_status, pointsA_status
        protocol
                (next_kind_of_train == STOPPING) --> setUPsignalclear(),
                (next_kind_of_train == THROUGH) --> setMsignalclear();
                ....
}

agent setUPsignalclear {
        handle homeMsignal_status, pointA_status, homeUPsignal_status
        protocol
                (pointsA_status == TO_MAIN) and (homeMsignal_status = CLEAR)
                        --> homeMsignal_status = DANGER;
                (pointsA_status == TO_MAIN) and (homeMsignal_status = DANGER)
                        --> pointsA_status = TO_PLATFORM;
                (pointsA_status == TO_PLATFORM) and (homeMsignal_status = DANGER)
                        --> homeUPsignal_status = CLEAR
}

agent setMsignalclear {
        handle homeMsignal_status, pointA_status, homeUPsignal_status
        protocol
                (pointsA_status == TO_PLATFORM) and (homeUPsignal_status = CLEAR)
                        --> homeUPsignal_status = DANGER;
                (pointA_status == TO_PLATFORM) and (homeUPsignal_status = DANGER)
                        --> pointsA_status = TO_MAIN;
                (pointsA_status == TO_MAIN) and (homeUPsignal_status = DANGER)
                        --> homeMsignal_status = CLEAR
}
```

It's possible to regard the `setUPsignalclear` and `setMsignalclear` agents as roles for the signalman. This would be most plausible if achieving the "neutral" / "safe" state of readiness, when both home signals are set to danger, was acknowledged as a separate role (introducing a "`setupsignalssafe`" agent). Note further that the notion that the next train to arrive is a stopping train is merely a motivation for the intelligent and conscientious signalman to prepare the station for its arrival. As the circumstances of the accident show, there is nothing to oblige the signalman to adopt what is necessarily the most appropriate role (in principle, the signalman could decide to set both signals to DANGER and take the day off). Neither can the timing of the signalman's actions be considered in isolation from the real situation: as the accident revealed, in some circumstances, setting the home signals to DANGER was not an adequate precaution against disaster, as there was insufficient time to bring the train safely to a stop. And quite obviously, the changing of the status of signals and points is not something that could be synchronised arbitrarily with the passing of a train etc.

The above discussion is relevant to one aspect of the accident scenario, though it doesn't take account of the role of the gong and disc protocol within the operational framework (a rather controversial issue in the BoT report, since E and H gave conflicting evidence about the communication procedures followed). To account for another very significant aspect of the situation: the failure of E's watch, we also need to refine the idea of `next_train` as a function of the time (`timenow`) and the schedule:

```
agent signalmanE {
        oracle
                timenow
                next_train, home1signal_status, home2signal_status, pointB_status
        derivate
                next_train is f(timenow, schedule)
                next_kind_of_train is typeof(next_train)
                status_or_next_train is
                        f(next_kind_of_train, schedule)        // status is STOPPING or THROUGH
        handle homeMsignal_status, pointsA_status
        protocol
                (next_kind_of_train == STOPPING) --> setUPsignalclear(),
                (next_kind_of_train == THROUGH) --> setMsignalclear();
```

```
        ....
}
```

... where we ideally expect the signalman to know the current time:

```
agent watchH{
        state timenow
        derivate timenow is actualtime

}
```

Some fairly complex derivate or maybe procedural component is needed to determine whether next_train is STOPPING or not (probably routinely defined by a dependency if the schedule is being followed in normal operation). (The BoT report refers to the fact that "Notice by telegraph was, indeed, received at the Tamworth station of the approach of the Irish mail train in advance of the goods train; but this notice was not communicated to the signalman ...".)

Anomalous situations

The above discussion raises the issue of non-standard contexts. Already have such an issue to consider in connection with the unreliable watch. Deal with this by attributing different roles to the watch - the classification of observables becomes dependent on context.

For a watch, have two contexts - watch can be going or stopped.

```
agent watchH {
        state timenow, status (= GOING, STOPPED)
        agent watchHgoing {
                state           error (= +/- n seconds )
                derivate        timenow is time + error
                                        ## watch could be slow or fast
                                        LIVE is (status == GOING)
        }

        agent watchHstopped {
                state           timenow = time0
                derivate        LIVE is (status == STOPPED)
        }
}

agent watchHmech {
        handle status
        oracle powersourceOK
        derivate status is if (powersourceOK) then GOING else STOPPED
}
```

With a clockwork clock, might want to take into account the responsibility for winding it - and so invoke agency of signalmanH again here.

Actually (of course!) the roles of the signalmen are affected by whether there is or isn't a train present at the station. As in the case of the Railway Arrival-Departure Animation, it is necessary to instantiate some observables that are only meaningful if and when there *is* a train in the station.

```
agent train_at_station {
        state   position
                        speed
                        platform
        derivate
                        LIVE is f(position, ...)
                        ## "at station" might mean between points A and B, or perhaps
                        ## should mean between points A and the distant signal
                        ## cf observable 'engaging' that features in the Railway Station Animation
}
```

Can now frame roles for the signalmen according to whether trains are present or not etc., bearing in mind that there may be more than one train present at the station at any one time. Something more complex but along the lines of the account of watch roles is what's needed here.

There are aspects of the analysis of the accident scenario that provoke reflections about possible actions that might not be part of the training manual. Perhaps signalman H could have diverted the express back on to the main track for instance, by shifting the points at B. (As the BoT report suggests, such a diversion might have worked in principle since the train successfully negotiated the points at A at a speed estimated at 45 mph, and was eventually travelling at about 15 mph. Even at that speed the momentum of a train was quite sufficient to cause catastrophe given the strength of the buffers and the proximity to the river bank etc.)

How could we model such an interventionary action on the part of H?

```
agent signalmanH {
        oracle  is_train_at_station
                        train_at_station
                        pos_train_at_station
                        speed_train_at_station
                        kind_train_at_station
                        ## could make into state observables of "train_at_station" agent
                        ## or better "train" agent "at station" here
        handle  pointsB_status
        privilege
                (kind_train_at_station==THROUGH) && (pos_train_at_station==PLATFORM_LINE)
                        --> pointsB_status = ...
}
```

Note the issues here about what signalmanH can observe. Does he know that the train on the PLATFORM_LINE is a THROUGH train: from the schedule? because it's going unusually fast? because he recognises that it is the Irish Mail? etc.

Might also ask - is he *supposed* to be able to observe such things? - i.e. is it part of his job description? If it were, then this would be a flaw in the railway system conception, since a train going the other way could interrupt his observation. A related question is: in what ways was the telegraph expected to enhance the communication between the two signalmen and improve upon the pre-existing gong and disc mechanisms?

The above discussion indicates how developing an ESD account can serve a purpose that is primarily provocative rather than functional, stimulating us to ask questions that might otherwise not occur to us. In general, the development of an account and an EM artefact may usefully proceed together. Such an exercise could be particularly useful if carried out in conjunction with a close reading of the BoT accident report at http://www.railwaysarchive.co.uk/documents/BoT_Tamworth1870.pdf, which includes additional detail about the precise distances between key points, the weather conditions, the gradients and slipperiness of the track, the composition of the train, including weights of the component vehicles, condition of the brakes, and the eye-witness reports from railway personnel both on and off the train.

Historic Railway Accidents 5

Abermule **January 26th 1921**

Abermule station is a small country station on the single-line Cambrian railway track from Whitchurch to Aberystwyth on the west coast of Wales. The neighbouring stations are Newtown to the West and Montgomery to the East. Trains can pass each other at Abermule, and the single-line sections of track between Montgomery and Abermule and Abermule and Newtown are protected by the Tyer electric tablet instrument (patented in 1878).

The Tyer instrument at station X resembles an automatic slot machine that is connected by telegraph to a similar machine at the next station Y along the line. A train travelling from X to Y has to receive an XY-tablet from the machine at X before it is authorised to go. The Tyer machines at X and Y ensure that an XY-tablet can only be released from either machine through synchronised action of the operators at X and Y. They are also electrically interlocked so that once an XY-tablet has been withdrawn at X, no XY-tablet can be withdrawn at Y until all the XY-tablets issued at X have been inserted in the machine at Y.

Abermule is manned by the stationmaster Lewis, the signalman Jones, and two young staff: the porter Rodgers and the ticket collector Thompson. The Tyer machine at Abermule is housed in the instrument room in the station building and not in the signal box. Only L and J are meant to use the machines, but in practice, all the staff do so from time to time.

The Accident

A stopping train that travels East-West from Whitchurch to Aberystwyth is scheduled to cross the West-East Aberystwyth-Manchester express at Abermule shortly before midday. The E-W train has just arrived at Montgomery, and the following sequence of events occurs:

- J at Abermule gives Montgomery clearance to release an MA-tablet for the E-W train to come forward. J establishes by telegraph that the express has left Moat Lane, the next station west of Newtown.

  L is at lunch, so only J, R and T know about this event.

- R at Abermule gives Newtown clearance to release an NA-tablet for the express to come forward.

  Only T is in the instrument room at the time, as L is in the goods yard, and J has gone to open the level crossing gates for the E-W train.

- R walks to the end of the platform opposite to the signal box to set the points for the express train to enter the passing loop. Before he gets around to this, he is distracted by the arrival of the E-W train.

  Had R set the points, he would have had to ask J to release the lock from the signalbox. In the event, the points are correctly set for the E-W train to leave and J is unaware that the express is expected.

- T meets the E-W train and collects the MA-tablet from the driver. T takes the tablet towards the instrument room, but meets L en route. L asks T where the express is, and T says "just passed Moat Lane". T then goes off to collect tickets and hands L the MA-tablet without further explanation.

  J does not know that the express is on its way. R doesn't expect the E-W train to depart yet. L assumes from his conversation with T that
  - the express is running late,
  - the tablet he has been given is the NA-tablet.

- L returns the MA-tablet to the driver of the E-W train believing it to be the NA-tablet. The driver doesn't check the identity of the tablet, and J signals the train on its way to Newtown.

The engine-men of the E-W train and 15 passengers are killed in the resulting collision. Its takes 50 hours continuous work by a breakdown gang to clear the line. The E-W breakdown train could not proceed from Montgomery to Abermule until the MA-tablet had been recovered from the wreckage. This tablet was discovered by the driver and fireman of the express, both of whom survived the crash with injuries.

Your agenda

a. What are the protocols and privileges of the various agents as laid down by regulation?
b. What are the protocols and privileges of the various agents as exercised in practice?
c. Analyse the knowledge each agent has at each stage as the events occur.
d. Analyse the knowledge that each agent should have had at each stage.
e. Analyse the assumptions the agents make in their communication.
f. Analyse the role that spatial distribution of agents plays in the events.

g. Can you work out what interlocking – recommended by the inquiry – would have prevented this accident? Would that have been foolproof?
h. What would have been the implications had the crew of the Express not been able to recover the MA-tablet?