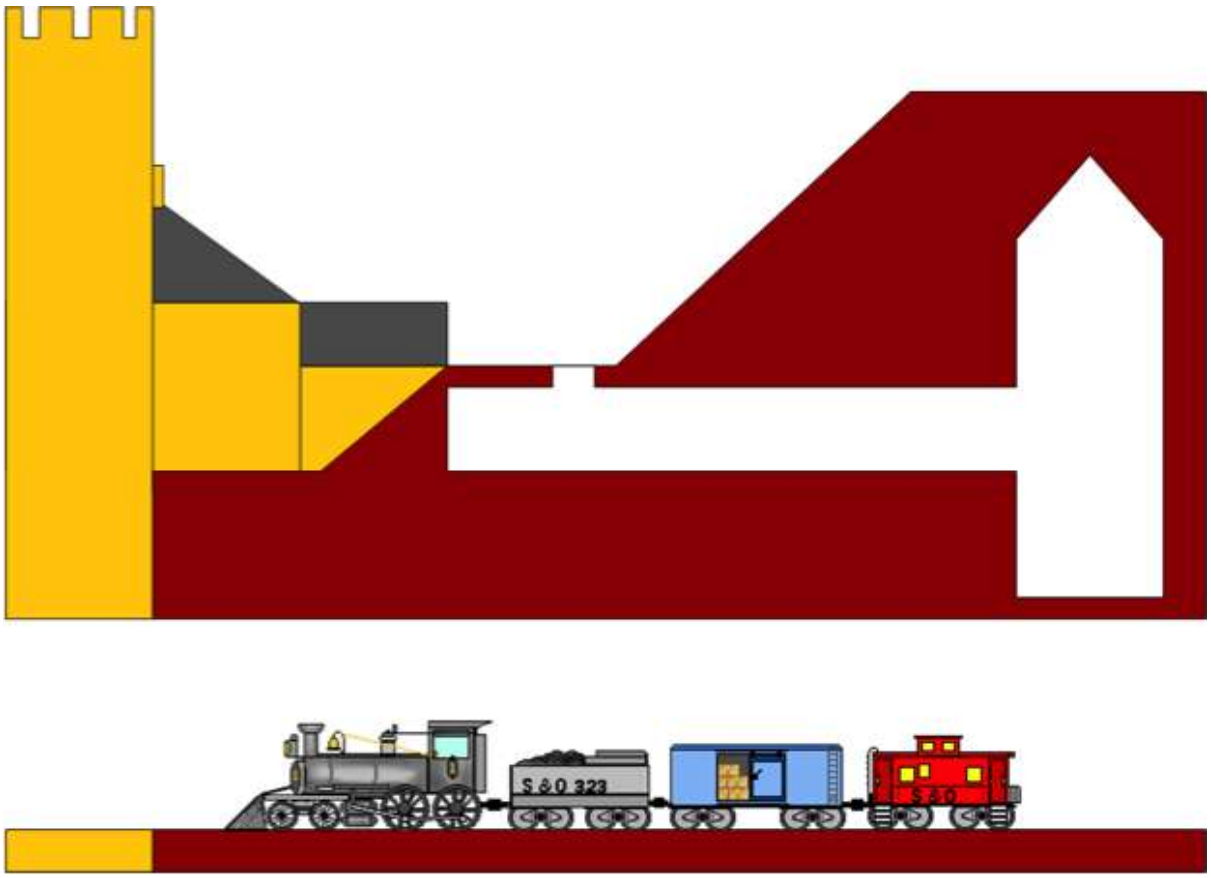
8/8/2013



CAMBRENSIS

THE CLAYTON TUNNEL CASE STUDY

An iDEPEND/ FRAM Test Case | David Slater

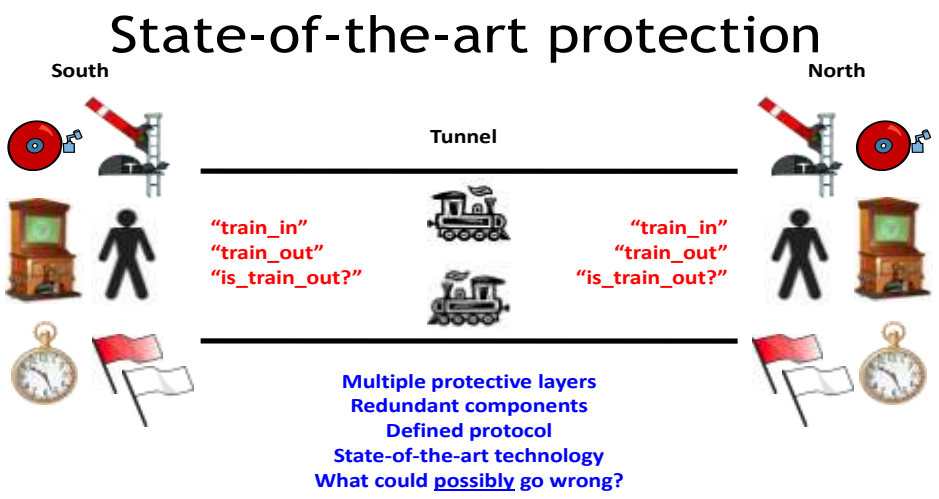
2

Overview

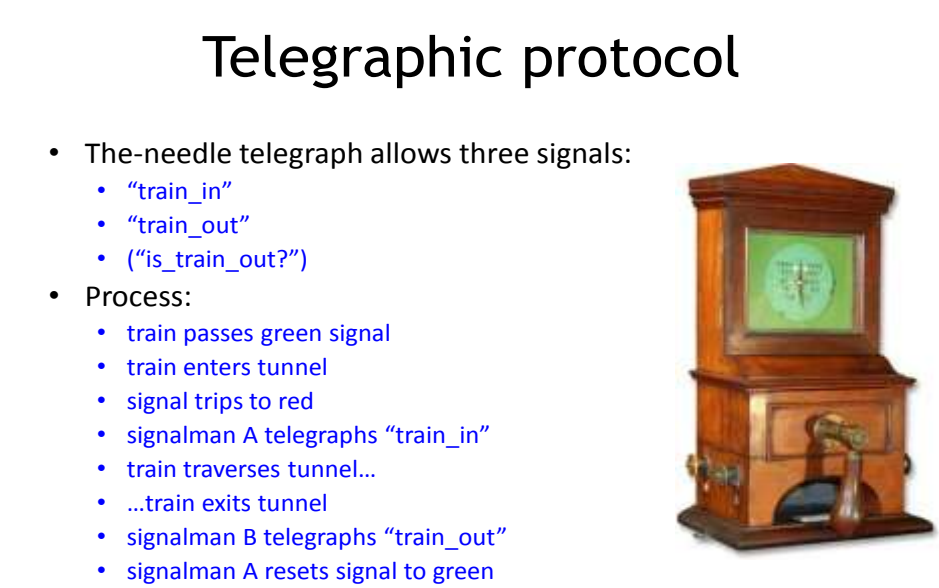
The **Clayton Tunnel rail crash**, which took place on Sunday 25 August 1861, five miles from Brighton on the south coast of England, was the worst accident in the British railway system to that time. Two trains collided inside the tunnel, killing 23 and injuring 176 passengers. The disaster scenario actually involved three successive northbound trains on the same track, which all left Brighton station within a few minutes of one another. The signalman at the south end of the tunnel tried to stop the second train from entering the tunnel before the first one had left it, but wrongly thought his red flag had not been seen, and then misinterpreted a telegraph signal from the north end of the tunnel as referring to the second train instead of the first. Assuming that both trains had cleared the tunnel, he signalled the third one to proceed, but in fact the second train was trying to back out.[1]

SYSTEMS/ FUNCTIONS IN OPERATION AT THE TIME

Signalman Henry Killick had an alarm bell linked to a signal, a needle telegraph and a clock in his cabin close to the south entrance of the tunnel. He could control the signal by a wheel in the cabin, but it would normally be at "danger" unless he approved a train to enter the tunnel. When a train passed, the signal returned automatically to "danger", but if it did not, the alarm bell would ring.



The needle telegraph instrument connects signalmen at the portals of the tunnel, and is used for both lines. The telegraph had been installed here about 1851, a typical date for the first use of the telegraph through long tunnels, on steep inclines and at junctions. The method of use is clearly explained below.



The telegraph was linked to the north signal box, and would show there was a train in the tunnel if the signalman at the other box activated it by pressing and holding down a switch. Otherwise the needle would hang vertically. A deflection of the needle to the left signifies 'train in,' and a deflection to the right, 'train out.' When a train enters the tunnel, the signalman displays Danger and sends 'train in' to the man at the other portal. When this train leaves, 'train out' is returned, and the signal turned to Safety. The signals are momentary, and may be interspersed with conversation or signals relating to a train in the other direction.

THE ACCIDENT SEQUENCE

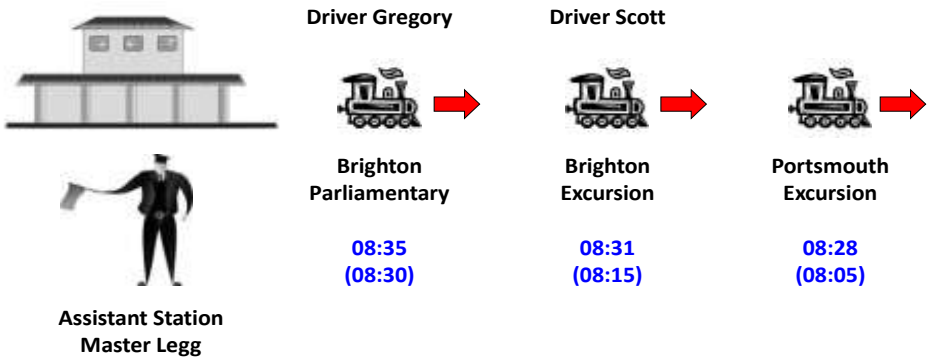
In modern parlance the horrific accident that occurred on 25 August 1861 would be said to have been "an accident waiting to happen". It was certainly a profound shock to the LB&SCR, as well as to railways in general, and what was further shocking in the Victorian mindset was the fact that the collision occurred on a Sunday.

Two excursion trains were due to set out from Brighton station ahead of a timetabled 8:30am departure. These two were a late-running Portsmouth to London train that had been due to depart Brighton at 8:05am and a Brighton to London train due to depart at 8:15am. In those days the LB&SCR was not known for its punctuality and the erosion of the time intervals between the trains was nothing uncommon. The line was worked on the time interval basis which was quite safe providing the Rules were strictly obeyed and the interval between trains sufficient for a Guard to protect his train in the event of any incident. Assistant Stationmaster Legg, realizing it was some six minutes after the due departure time of the 8:30 train, sensibly began dispatching them in their rightful sequence as the two excursion trains had a faster schedule than the ordinary train.

The time-interval system required trains on the same track to be separated by 5 minutes. On this day, the three trains actually left Brighton within 7 minutes of each other:

- Portsmouth Excursion left at 8.28 am
- Brighton Excursion left at 8.31 am
- Brighton Ordinary left at 8.35 am

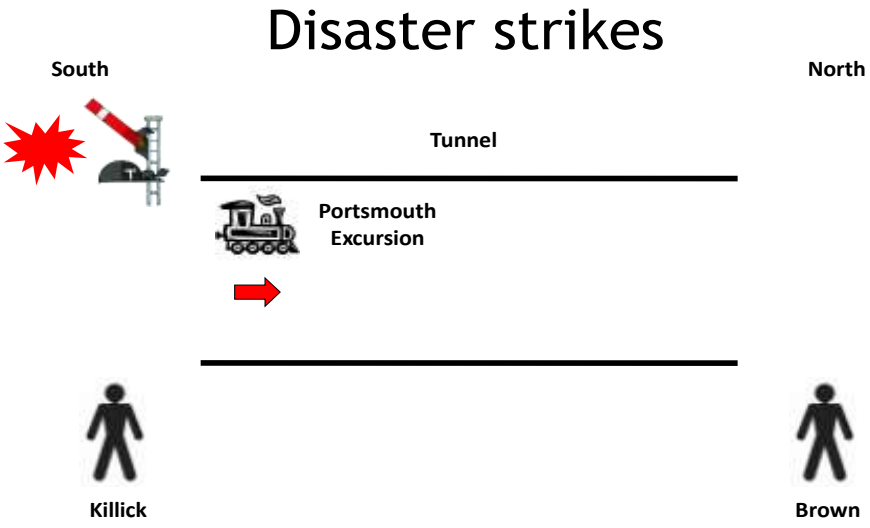
Although time interval was used on the open part of the route, the line within Clayton Tunnel was controlled by a block section, worked by the single needle telegraph and protected by a Whitworth automatic revolving banner signal. The automatic part of the title refers to the signal being replaced mechanically when a train ran over a treadle, requiring the Signalman to pull off the signal once more for the following train. In this location there was a Signalman at either end of the tunnel, each working a 12 hour shift, although in order to alternate between day and night shifts, it was the practice to work 24 hour shifts on Sundays! On the day in question the south side of the tunnel was signalled by Signalman Killick, whilst at the north end was Signalman Brown.



5

The first train to pass Signalman Killick was the Portsmouth excursion which passed over the treadle and continued on to enter the tunnel. At the tunnel mouth, this first train passed the signal at "clear". The "automatic" signal, however, failed to return to danger and the alarm bell rang to warn Killick

Killick sent a "train in tunnel" message to Brown in the north cabin, but did not return the signal to "danger" in time to stop the second train from passing the signal and travelling to the tunnel. It was only 3 minutes behind, and may well have caught up with the first train.

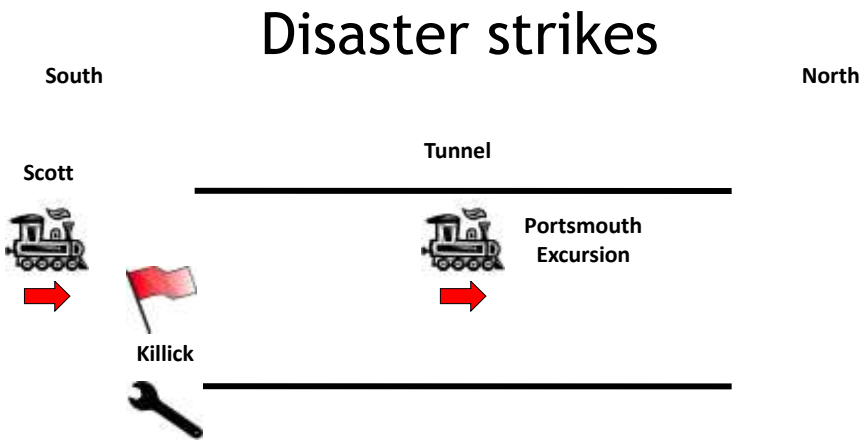


6

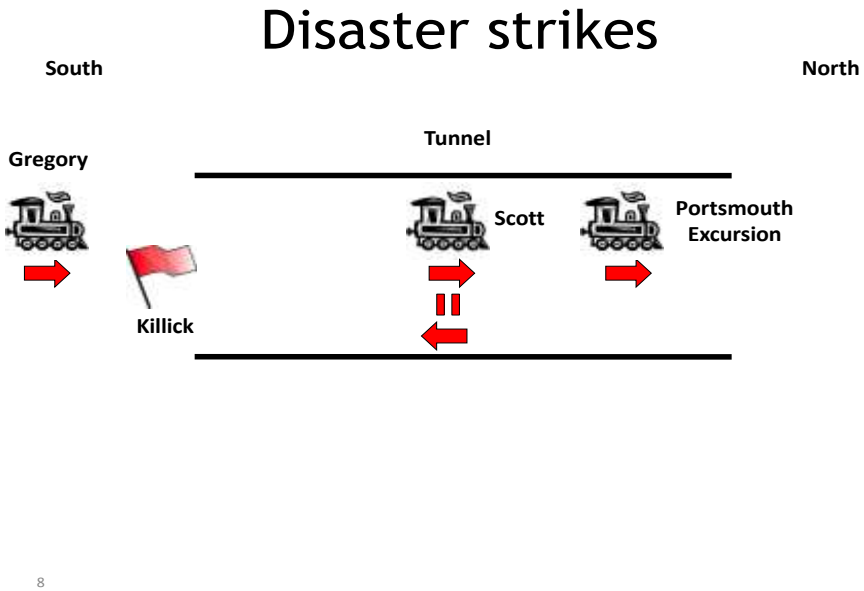
.

Realising that the first train was still in the tunnel, he had rushed out of the cabin waving his red flag to stop the second train just as it was passing. He could not be sure that the driver had seen

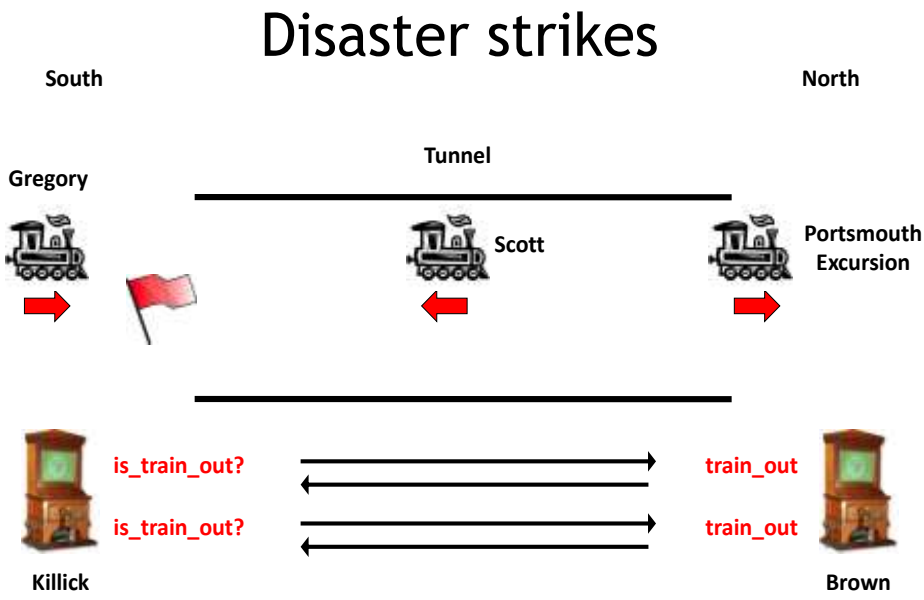
the flag. This second train had passed the signal, which was incorrectly showing a “proceed” aspect and which once again failed to return to danger. Killick having immediately displayed a red flag , as the train charged into the tunnel, did not know whether or not Driver Scott on Craven 2-2-2 Nº126 had seen it. He telegraphed Brown "is tunnel clear?" Scott had in fact, seen the flag, and realizing that the flag signal contradicted the Whitworth signal knew that something was wrong and stopped the train in the tunnel.



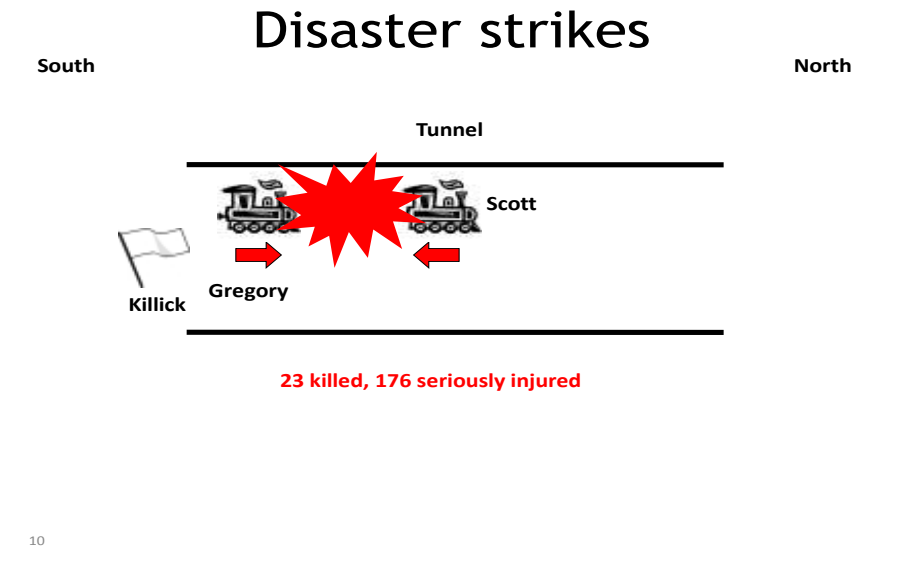
So far, so good, but now things started to go horribly wrong. Instead of staying put, with the Guard protecting the rear of the train, Scott decided to set back and propelled his train back towards the south end of the tunnel in order to speak to Killick.



At that moment, the first train cleared the tunnel, so Brown signalled back "tunnel clear" to Killick. But unfortunately, Killick thought that Brown was referring to the second train and not the first. In fact, as we know, the second train's driver having seen the red flag and stopped about half a mile into the tunnel, was then reversing back to return to the south end.



Meanwhile Killick now saw the third train approaching (and stopping at?) his signal;(was it now working correctly?) and, thinking that the tunnel was clear, he waved his white flag for it to proceed (reinforcing signal?)



The second and third trains then collided in the tunnel with great force. The second train was pushed forward, and the loco obliterated the guard's van at the rear before smashing into the

last carriage. It then rode up over the carriage roof and smashed its chimney against the tunnel roof before stopping. Many of the 23 deaths were in this last carriage, where passengers were burnt or scalded to death by the broken engine.

The crew of the second engine were lucky in that Driver Gregory sustained minor injuries whilst his fireman escaped injury altogether, and Gregory was commended for his prompt action which no doubt prevented a far higher death toll.

AFTERMATH

A nine-day inquest was held at Brighton town hall into the deaths of the 23 victims. But as if the accident wasn't bad enough, this subsequent Inquiry descended almost into farce

The jury did not find any negligence by either the south end signalman, Killick or Brown.[2] Killick, was not held responsible so wasn't charged[1]; but Assistant Stationmaster Legg was judged to have acted recklessly in dispatching the trains too close together (against the rules of the company); and was charged with manslaughter. Legg was committed for trial, but found not guilty.[3] When he appeared at Lewes Assizes, the jury threw out the indictment.

As for his “top” Manager, Craven, who had a very bad reputation in the way he treated his men, he would defend his department fiercely and on this occasion got away with protesting that Scott's action in setting back his train was quite in order!

The Board of Trade inspector, one Captain Tyler, concentrated his attention on the time interval method of working, the Railway put up the counter case that better mechanical safeguards would be self defeating as they would lead to the men being less alert and emphasized that this accident was caused by the failure of a mechanical safeguard.

One other aspect of this accident noted was that Signalman Killick was working a continuous 24 hour shift that day, rather than the regulation 18 hours in order to gain a complete day off duty.

In his report on the accident Captain Tyler stated that " it was disgraceful that a man in so responsible a position as Signalman Killick should be compelled to work for twenty-four hours at a stretch in order to earn one day of rest a week."[4]

The ultimate blame for the accident though, was placed on 'Traffic'; with Captain Tyler recommending the adoption of absolute block working, and continuous brakes. The Railway did nothing about the recommendation at this time.

The incident then passed into railway history as Britain's worst ever railway accident, until the Irish Mail disaster some six years later. The catastrophe publicised the problem of trains travelling too close together, with signalmen having to appraise the situation too quickly for safety's sake. A simple communication mistake between the two signal boxes caused havoc that Sunday, but the telegraph was also blamed for the tragedy because it did not register without continual pressure on the switch. The signal, too, was also at fault for not returning to "danger" immediately after the train had passed. The accident encouraged the use of the block system (rather than the time interval system) for the remainder of the railway system.

INSIGHTS

They asked the Classic question

What was the **CAUSE?**

And produced the same standard answers which you would get today (depending on whose doctor is spinning!)

- **HUMAN ERROR** – signalman, Driver, Asst Stationmaster?
- **Equipment Malfunction** - Telegraph, Signal?
- **PROCEDURES?** - SPAD's**?**
- **"ROOT" CAUSES?** – Shift length/ time off policy, Communications?, lack of leadership/ management failure?
- **"SWISS CHEESE HOLES? -**
- **TRIPOD/ TAPROOT CHECKLIST?, etc.**

Or is there a more objective and constructive approach?-

e.g. was it the **TIME ELEMENT**, which to be fair they commented on also?

- Signalman's reflexes dulled (24hr shift?)
- Station Master not observing time slots – (not important? Or Target pressures?)
- Time taken to react to alarms and operate telegraphs in emergency too long
- **No automatic procedure for SPAD's** (Signal passed at danger?)
- **Uberlingen response from drivers** - one believes signal / one backs out because he's not sure?
- **Not enough resilience (foresight?) in the system**?

All this is easily demonstrable if only they had had a way of simulating the dynamics of the situation and the foresight to run emergency exercises, not a common practice in those days before Health and Safety!

They have only partially realised the missing insight, the dynamic interaction of these functions that throws up a situation where the timing is insufficient for the adaptation of intelligent operators to a previously unknown combination of circumstances (a Black Swan?) Here it has "engineered?" an unfortunate system crash. But they did not learn the lesson here as in many other cases where system complexity has soundly defeated native wit. After all they were only human!

This was then, as many accidents were/are, a classic example of a combination (resonance?) of a sloppily-designed system, mechanical error and human fallibilities.

SIMILAR ACCIDENTS

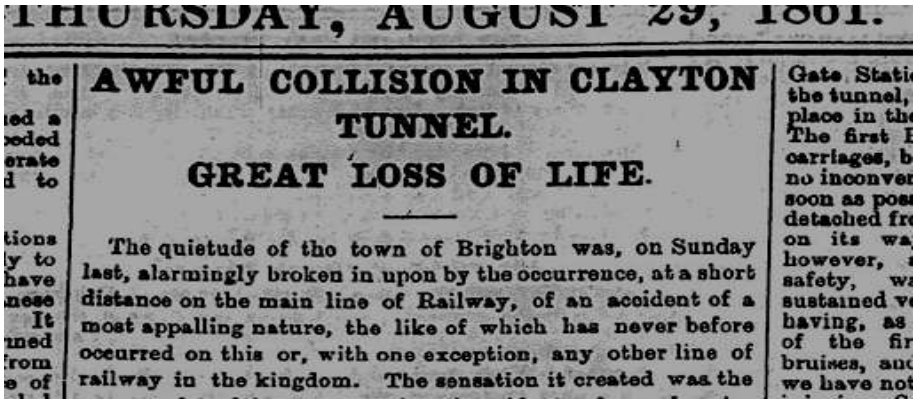
Other accidents in which the signalman forgot, or got confused about, the presence of a train include:

- Welwyn Tunnel rail crash – 1866
- Thirsk rail crash – 1892
- Hawes Junction train disaster - signalman forgets about light engines on line - 1910
- Quintinshill rail crash - signalman forgets about train on line - 1915
- Winwick rail crash - 1934

POSTSCRIPT

Charles Dickens probably based his story "The Signal-Man" on this accident, dramatising the events (especially the bells and the telegraph needle), as well as adding other incidents. His own experience at the Staplehurst rail crash may have inspired him to write this ghost story. Readers of the story in December 1866 would likely have still remembered the Clayton accident.

23 killed, 176 seriously injured



THURSDAY, AUGUST 29, 1861.

AWFUL COLLISION IN CLAYTON TUNNEL.

GREAT LOSS OF LIFE.

The quietude of the town of Brighton was, on Sunday last, alarmingly broken in upon by the occurrence, at a short distance on the main line of Railway, of an accident of a most appalling nature, the like of which has never before occurred on this or, with one exception, any other line of railway in the kingdom. The sensation it created was the

11

AN ADDITIONAL GHOSTLY POSTSCRIPT,

David Porter (a Cambrensis Associate and Dependency Modeller to whom I am indebted for the extent of the details in this Test Case), lives in the house above the Tunnel entrance (www.claytontunnel.com). He says, "I never stay here on the night of 25th August (the anniversary of the train crash) because it's just a little too spooky!"

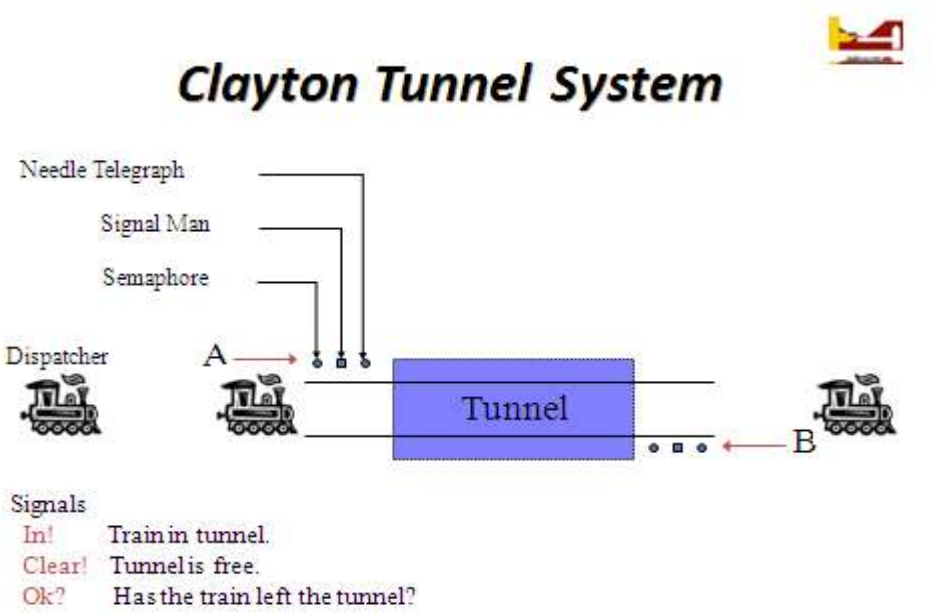
"The rear bedroom in this place has a bit of an atmosphere about it and tends to get cold around the anniversary of the crash.

I found out that some bodies from the crash were laid out in that particular room and also the rear garden.

There is also a hidden horizontal passage (adit) behind the cottage that intersects with a vertical shaft that goes down into the tunnel. The ghosts of the dead from the accident are said to frequent this passage…"

SO COULD WE DO ANY BETTER?

This is a classic scenario where a system has been designed to function mechanically like clockwork, provided all the parts work as they are supposed to. (Reliably?). To the Victorian determinists, the involvement of humans was OK provided they too worked like automatons. (Stayed on the script). Then this system is simple, predictable and safe?



But in real life, people are not automatons; the outside world impinges in many intrusive and disruptive ways. So the system needs to be recognized as real world and complex (even though it looks simple!)

So if we take an objective (agnostic?) view, systems are groups of functions carried out by components, human and mechanical. (Football teams rather than Rosary Bead Strings). If we accept that because they involve real people, they are necessarily complex; and hence we will never be able to completely understand, or predict behaviour, in dynamic, sociotechnical systems.

One pragmatic approach is to observe and see where variability (deviation from expectation) occurs; and then design in some resilience in the Functions to cope with it. But this observation needs a structured methodology to be able to identify, measure and develop capacity correctly to cope with these variabilities and deviations.

One approach to "modelling " (intended)functions rather than (failure)of components is Structured Analysis and Design Technique (SADT) which looks at software as an "Orchestra" of interacting "Functions" for playing "scores" of music

These exchange inputs and outputs with a range of other "Functions" .

Hollnagel has proposed to utilise and extend this approach to systems as a collection of these "Functional" units, he calls FRAM's. For each FRAM he defines a number of inputs and outputs necessary for the functions to interact.

FRAM IDENTIFICATION OF FUNCTIONS

For the Clayton Tunnel system then we have a number of these "Functions", all needing to interact correctly to enable the system to deliver "safe operation"

- Dispatcher (1)
- Driver (3)
- Semaphore Signal (1)
- Signal Man (2)
- Needle Telegraph (1)

We can then develop each of these functions into FRAM Modules (using Hollnagel's Protocols)

1. ***"Identify essential system functions***, using normal or accident-free performance as a baseline. This characterises each function separately but does not try to arrange or order them in any way. The starting point may be existing task analyses, procedures, expert knowledge, etc. The characterisation uses the following six aspects:

- **Input (I):** that which the function processes or transforms or that which starts the function,
- **Output (O):** that which is the result of the function, either an entity or a state change,
- **Preconditions (P):** conditions that must be exist before a function can be executed,
- **Resources (R):** that, which the function needs or consumes to produce the output,
- **Time (T):** temporal constraints affecting the function (with regard to starting time, finishing time, or duration), and
- **Control (C):** how the function is monitored or controlled.

Each function may be described by a simple table, which then can be used for the further analysis. It is also possible to show the functions graphically using a hexagon to represent each function

FUNCTION NAME	Station Master Legg
FUNCTION DESCRIPTION	Release Trains
INPUT (That which activates the function and/or is used or transformed to produce the output. **Constitutes t**he link to upstream functions.)	Timetable Prompt
OUTPUT (That which is the result of the function. Constitutes the links to downstream functions.)	Release Train
PRE-CONDITIONS (System conditions that must be fulfilled before a function can be carried out.)	All Clear from Signal Men
RESOURCES / EXECUTION CONDITIONS (That which is needed or consumed by the function when it is active (matter, energy, competence, software, manpower)	Competence
CONTROL (That which supervises or regulates the function. E.g., plans, procedures, guidelines or other functions.)	Region?
TIME (Temporal aspects that affect how the function is carried out (constraint, resource).	Timetable

Background function			
Foreground function			
	Timing	Precision	Elaborated
Potential variability			
Actual variability			

2. ***Characterise the observed variability of system functions***, considering both actual and potential variability. The purpose of FRAM is to provide an explanation of the accident in terms of combinations of performance variabilities. The second step is therefore for each function to describe the actual variability during the accident. This may point to other functions that must be characterised as part of the explanation. For instance, if the input to a function came too late, or was of the wrong kind, then the source of that input – i.e., another function – must be described and characterised. This may in turn require yet other functions to be described, until the total scenario has been accounted for.

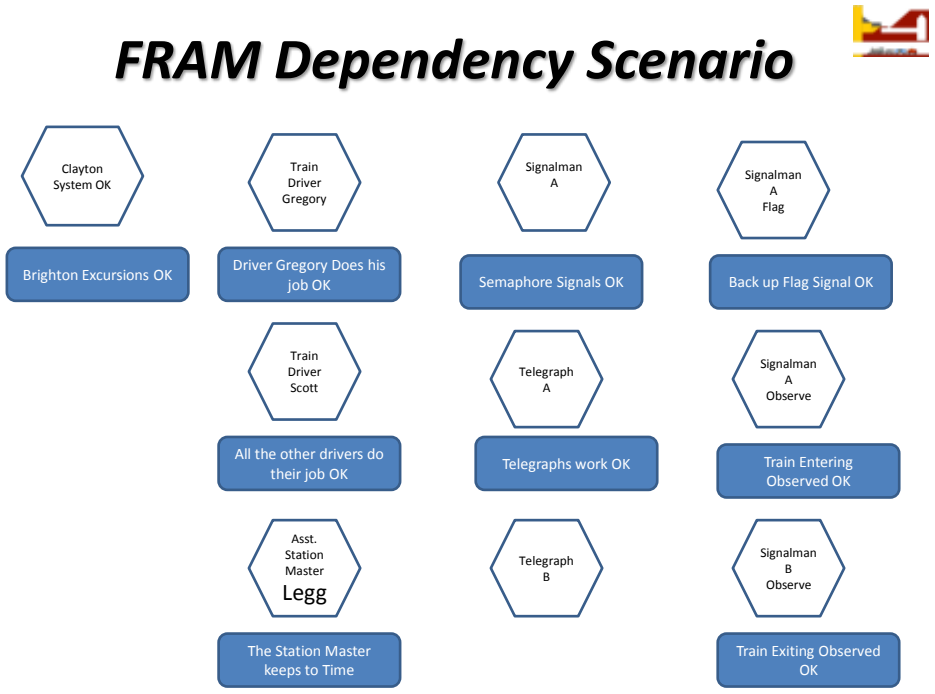
3. ***Identify and describe the functional resonance*** from the observed dependencies / couplings among functions and the observed performance variability. The output of the first and the second steps is a list of functions each characterised by two or more of the six aspects. (Notice that a function may require several instances of an aspect to be described.) The dependencies among functions can be found by matching or linking their aspects. For example, the output of one function may be the input to another function, constitute a resource, fulfil a pre-condition, or enforce a control or time constraint. The result is an overall description of how the functions were linked or coupled in the accident scenario, and therefore of how functional variability propagated through the system. In general, the links specify where the variability of one function may have an impact, or how it may propagate. Many such occurrences and propagations of variability may create a resonance effect: although the variability of each function may be below the normal detection threshold, they may in combination become a 'signal', hence constitutes a risk. This step may be supported by a visualisation of how the functions are linked. The visualisation can be valuable in tracing functional dependencies, but the analysis should nevertheless be based on the description of the functions rather than on the graphical representation.

4. ***Identify barriers for variability*** (damping factors) and specify required performance monitoring. Barriers are means to prevent an unwanted event from taking place, or to protect against the consequences of an unwanted event (Hollnagel, 2004). Barriers can be described in terms of barrier systems (the organizational and/or physical structure of the barrier) and barrier functions (the manner by which the barrier achieves its purpose). The four fundamental barrier systems are: (1) physical barrier systems that block the movement or transportation of mass, energy, or information; (2)functional barrier systems that set up pre-conditions that must be met before an action (by human and/ or machine) can be undertaken; (3) symbolic barrier systems that are indications of constraints on action that are physically present; and (4) incorporeal barrier systems that are indications of constraints on action that are not physically present.

Besides recommendations for barriers, a FRAM analysis can provide the basis for recommendations on how to monitor performance in order to detect excessive variability. Performance indicators may be developed both for functions and for the couplings between them".

ASSEMBLING THE INTERACTING FRAM'S

One of the ways to do this is to use "Dependency Modelling" (The Open Group Standard C 133, 2012) to provide a quantitative structure which shows the probable extent of the criticality of these dependencies (of the functions. This quantitative mind mapping tool, facilitates the interaction of common inputs and outputs. But which now can also import external inputs and outputs from outside the system to see the predicted effect on system behaviour

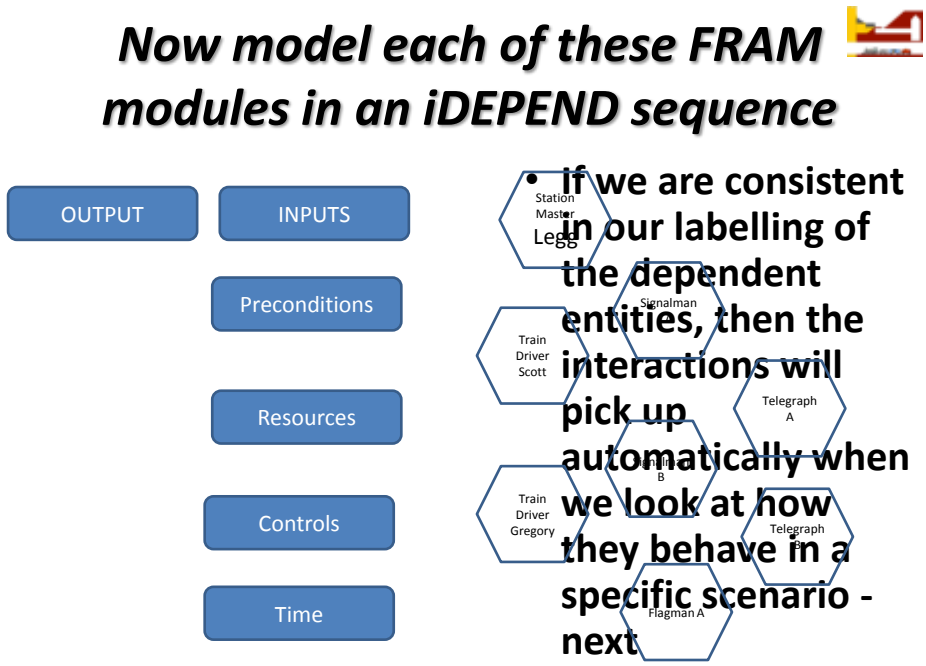


This gives us ten functions/ activities which are ongoing, interactive and interdependent in this particular system. We can list them below and model as separate models in an iDEPEND "Organisation". Initially we can concentrate on the interdependencies.

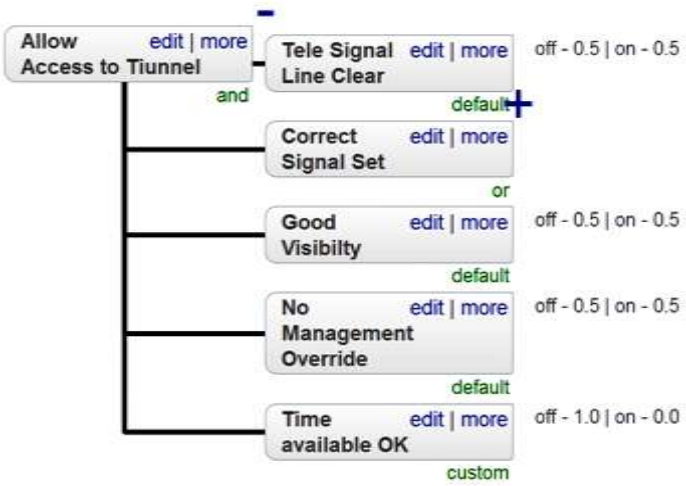
Function	**Description**	**Fore ground**	**Back ground**	**Type**	**Varia bility**	**Barr iers**
Dispatch	Control Release and Timing of Trains			Human		
Input	Train Ready					
Output	Signal Go					
Precondition	Line Clear					
Resources	Train Ready					
Control	Timetable, Slots					
Time						

Driver A	Control Train A's Movements			Human		
I	Signals Go					
O	Advance Train					
P	Line Clear, Go Signals					
R	Working Train					
C	Emergency Override					
T	Slots, Timetable					
Driver B	Similar			Human		
I						
O						
P						
R						
C						
T						
Driver C	Similar			Human		
I						
O						
P						
R						
C						
T						
Signalman A	Control S-N access to Tunnel			Human		
I	Telegraph Signal line clear					
O	Signal Driver Go					
P	Line Clear					
R	Working Signal, backup Flag					
C	Alarm					
T	Before Train enters Tunnel					
Signalman B	Observe Train Exits from Tunnel			Human		
I	Request from Telegraph					
O	Send Telegraph Message					
P	Observed Train Exit					
R	Working Telegraph, Visibility					
C	Query from Telegraph					
T	Time Elapsed					

	Sufficient					
Telegraph A	Signal Line availability			Tech		
I	Signal from B					
O	Signal to B					
P	Signalman operates					
R	Circuit, Power					
C	Operator					
T	Speed of response					
Telegraph B	Similar			Tech		
I						
O						
P						
R						
C						
T						
Signal A	Two position Semaphore			Tech		
I	Signalman A lever					
O	Move to other position					
P	Visibility good					
R	Working mechanism					
C	Treadle and Lever					
T	Speed of response					
Alarm A	Indicate Signal condition			Tech		
I	Change Signal position					
O	alarm					
P	If not moved in response to I,					
R	Working circuits, power					
C	Signalman					
T	Speed of response					



For example, one of the key activities/functions is that of Signalman A (Killick). This function controls access to the Tunnel by communicating by signals, the state of the line ahead as confirmed by signalman B using the telegraph. An attempt to model this function on the FRAM template might look like this:-



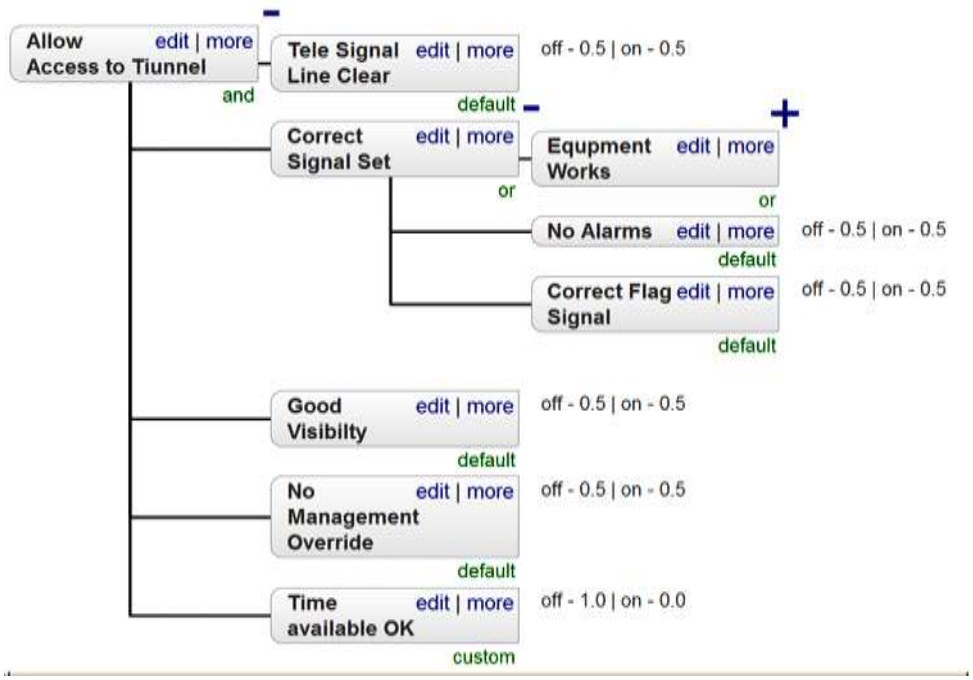
The I**nput** tele signal Line Clear is obviously an **Output** from Function Signalman B for that track. (The roles would be reversed for the other track).

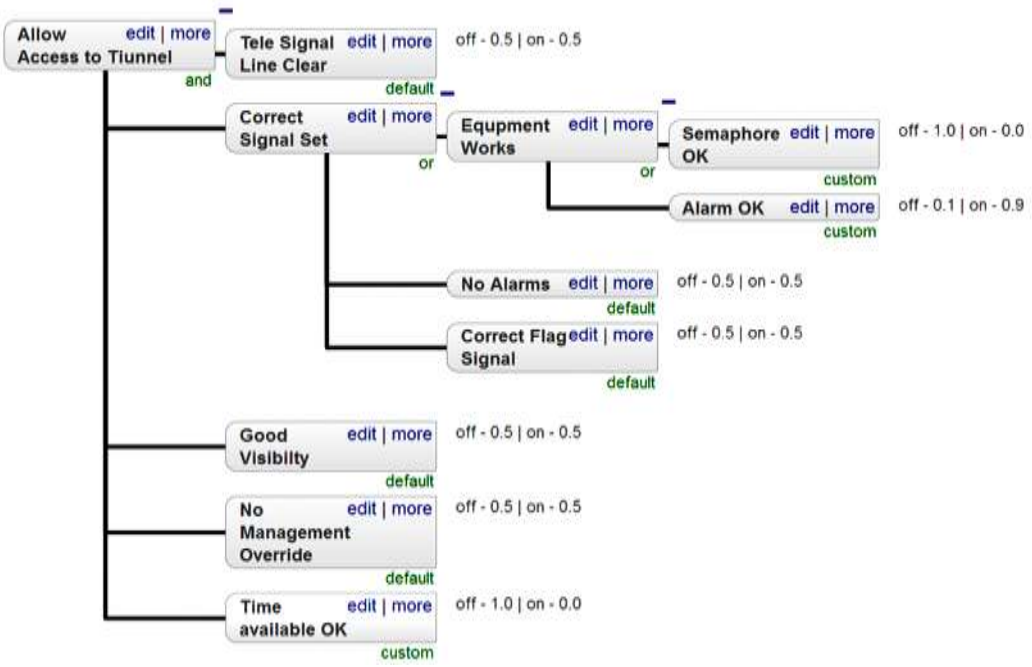
Correct signal set is determined by his own equipment and is a **Resource** condition?

Good visibility must be a **Precondition** as fog signals would be used in that contingency.

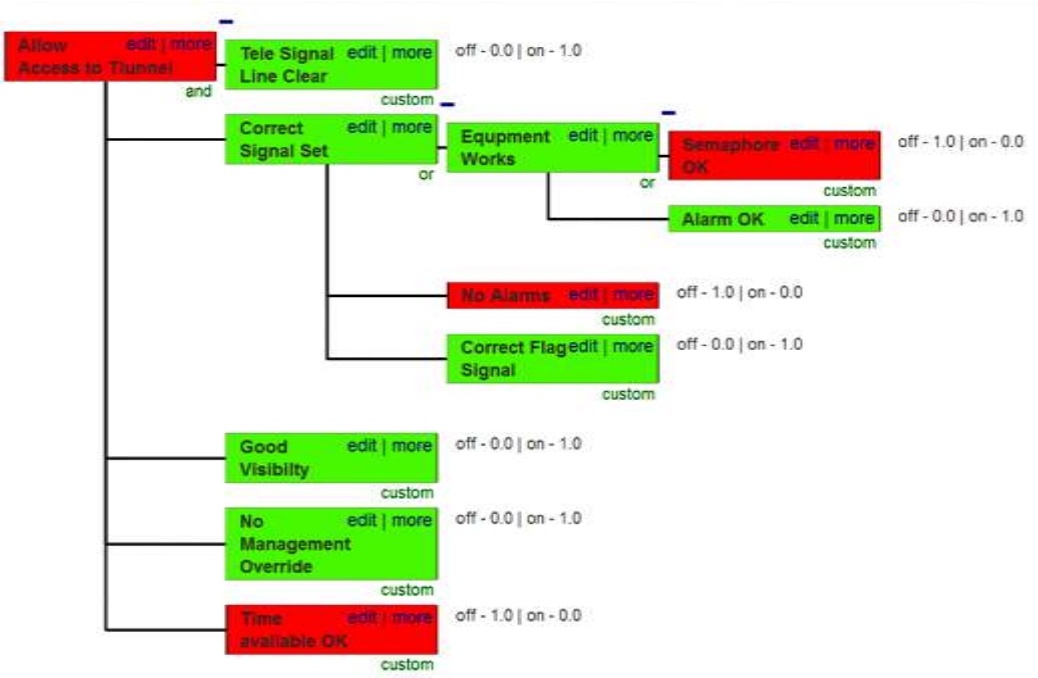
The interesting dependencies are **Control** (of which I suppose written procedures and Policies qualify were no doubt in place - When all else fails read the instructions?) and **Time** available for carrying out the prescribed actions.(for example as in the New York Aircraft Ditching, there was only time to get to page 3!).

So if we develop the Dependency "tree" and put in some numbers we see that **Time** is indeed the thing that can negate all the other contributors.





We can show this dynamically as red/ green probability bars (yes/no), which allow us to test the effect of varying these input and output probabilities to see the effect on the output of this function. So if for example the time available – i.e. time between trains is less than a critical duration – say 3 minutes, the system will not function as designed.



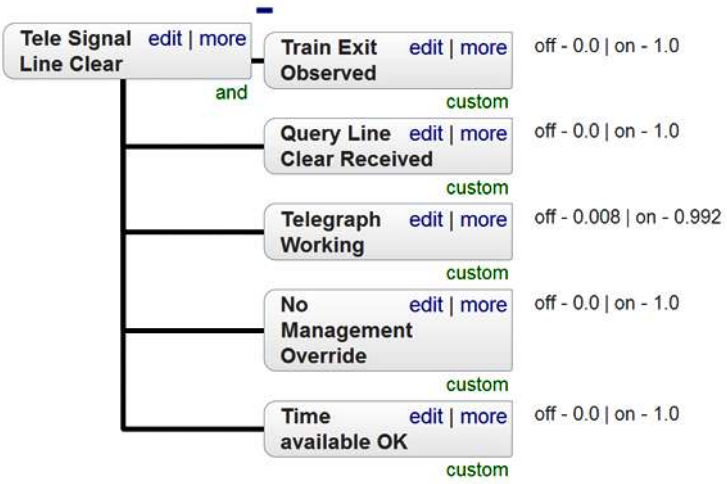
We can similarly model all the FRAM functions and run the same variability/ sensitivity tests to see the effect is.

We have not at this stage included external feeds, although "Visibility" is an obvious candidate and could be imported, or set.

The next stage is to model a second related Function - Signal Man B. Here each signalman has identical functions – one for the up track and one for the down track. So we take the subservient of the two for B.

His key responsibility is to determine whether the track is clear. He knows there is a train in from A and observing its exit can telegraph A that the Tunnel is now empty. Crucially this assumes only one train at a time is entering the tunnel.

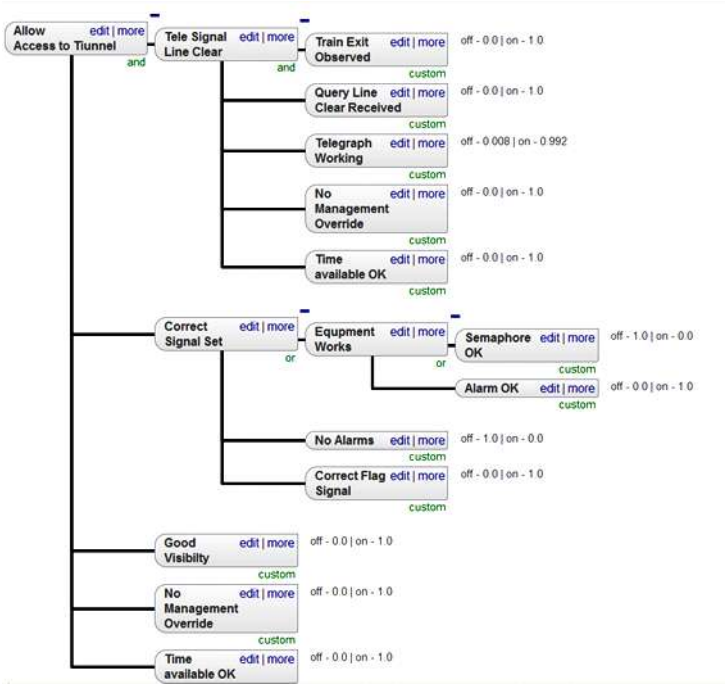
What happens if there are two – don't know – not in the book – not possible as designed? The function Signalman B is now modelled to reflect the procedures as specified.



As they are modelled as part of the same organisation, the entities are common and have to be carefully labelled to avoid the wrong ones being picked up incorrectly by the other models.

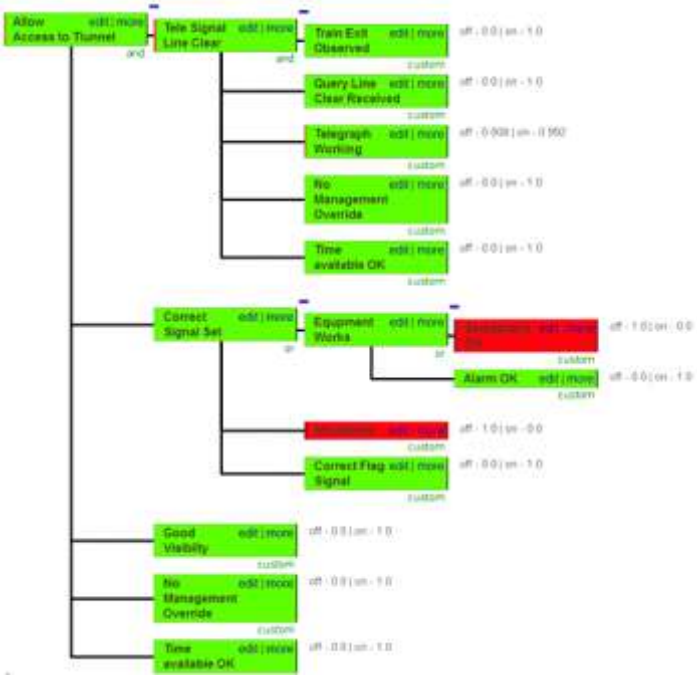
Conversely, if we have been systematic in our labelling, the models can pick up unexpected or unplanned dependencies. This is particularly pertinent once we include spatial or socio/ environmental factors.

So we can illustrate this by looking at a system with two models, “Signalmen A and B”. We can then see that the tool links these two functions together as shown below..



Now we can query the implications of different missed inputs, etc. on the combined “mini” system.

For example, if we set the time available to sufficient for both signalmen to perform their functions, , the system works as designed and access is successfully controlled, in spite of a semaphore signal failure.



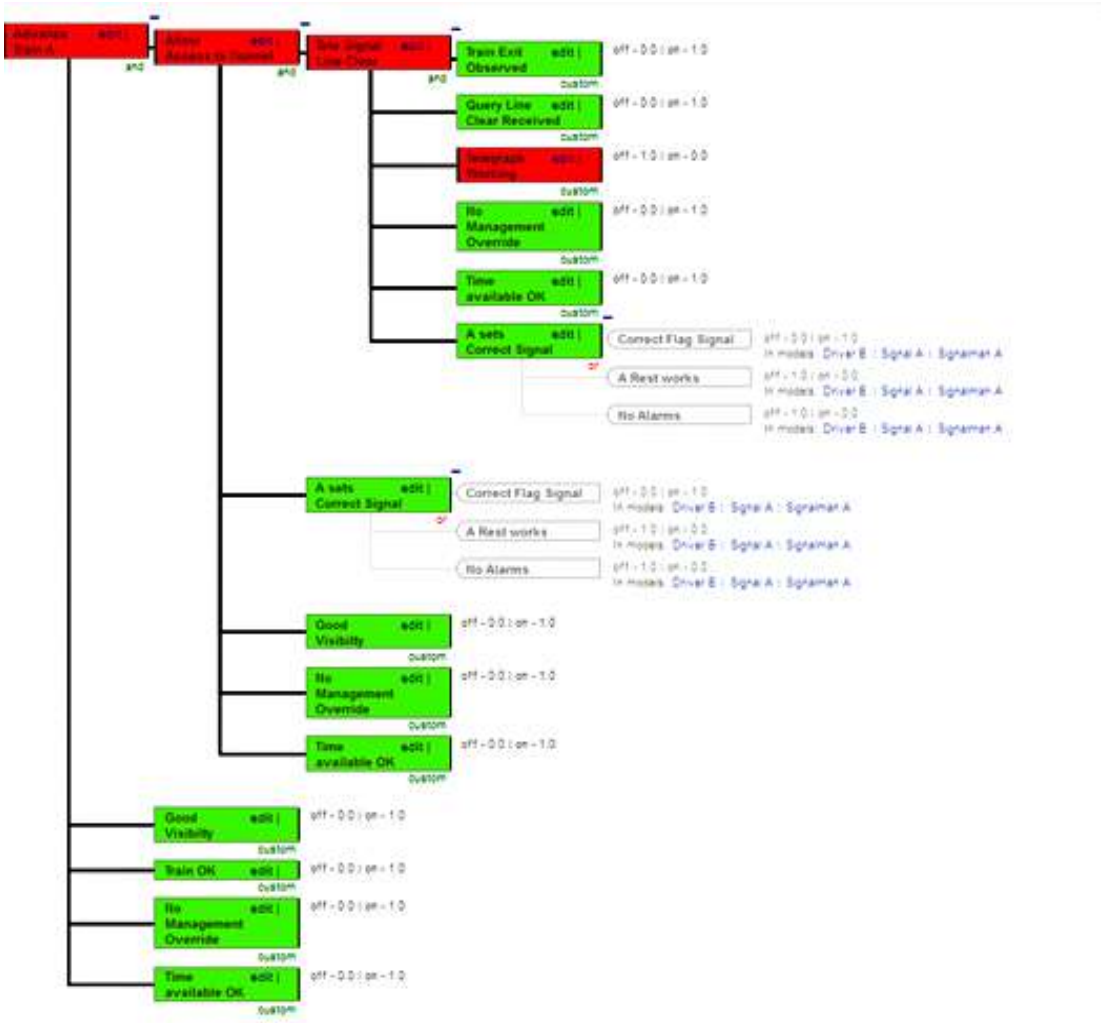
The next step is to model all the “actors” and see how they interact. The system now includes:-

- Dispatcher
- Drivers A, B and C
- Signalmen A and B
- Telegraphs A and B
- Alarm A
- ?

We can then see that time is still the common cause of failure for the functions involved. But we can now explore the effect of different functions – for example , the Telegraph. Obviously unavailability of either A or B makes the Telegraph function fail.

But the result is clearly crucial as there is no other way of communicating line status between the signalmen and hence the system fails.

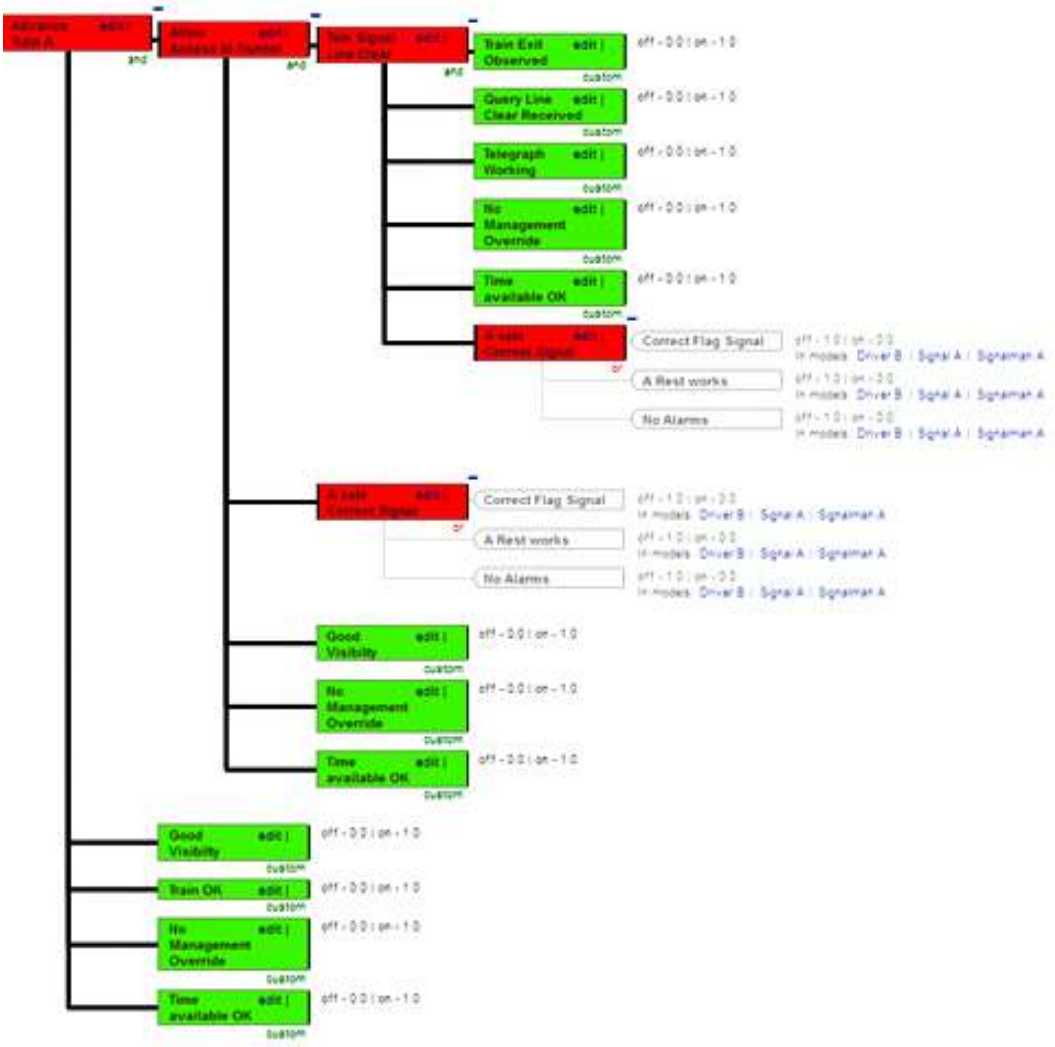
The example below is looking at the effect of the telegraph failure on the ability of Driver A executing his function to advance safely.



Another illustration is to look at the effect of Killick (Signalman A) showing the wrong Flag signal. This is input into the signalman A model – incorrect Flag. The driver will advance but not safely and the driver C function picks this up - that the Signalman A function is now not working correctly.

In fact all of the driver functions pick this up and cannot advance safely.

The Driver A example is shown below.



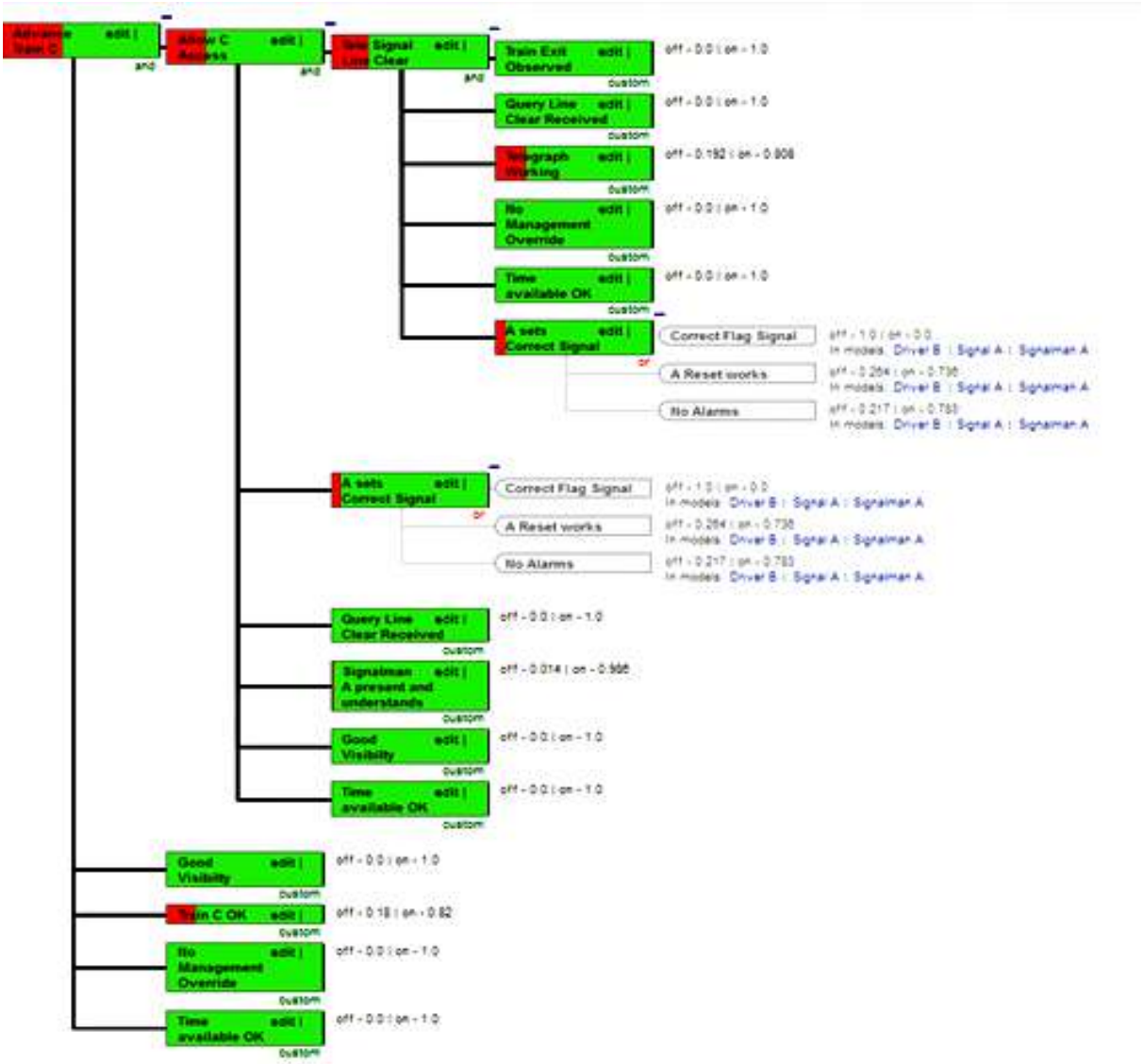
Looking at failure modes, by tracking the effect of failed functions on other functions is therefore quite straightforward.

But the tool allows us to also so apply it in predictive mode and assign probabilities to the various dependencies. Then as in the FRAM analysis we can systematically wary these to see to effect on the other functions.

This is a typical “What if” application of the dependency modelling approach.

As an example we can put in probabilities for the expected availabilities of the mechanical components (Signals, alarms, etc.).

This will give us an indication of how well the system could be expected to perform with infallible people operating it.



This is more clearly shown by running a sensitivity Analysis. The tool produces the 3 point sensitivity plot below.

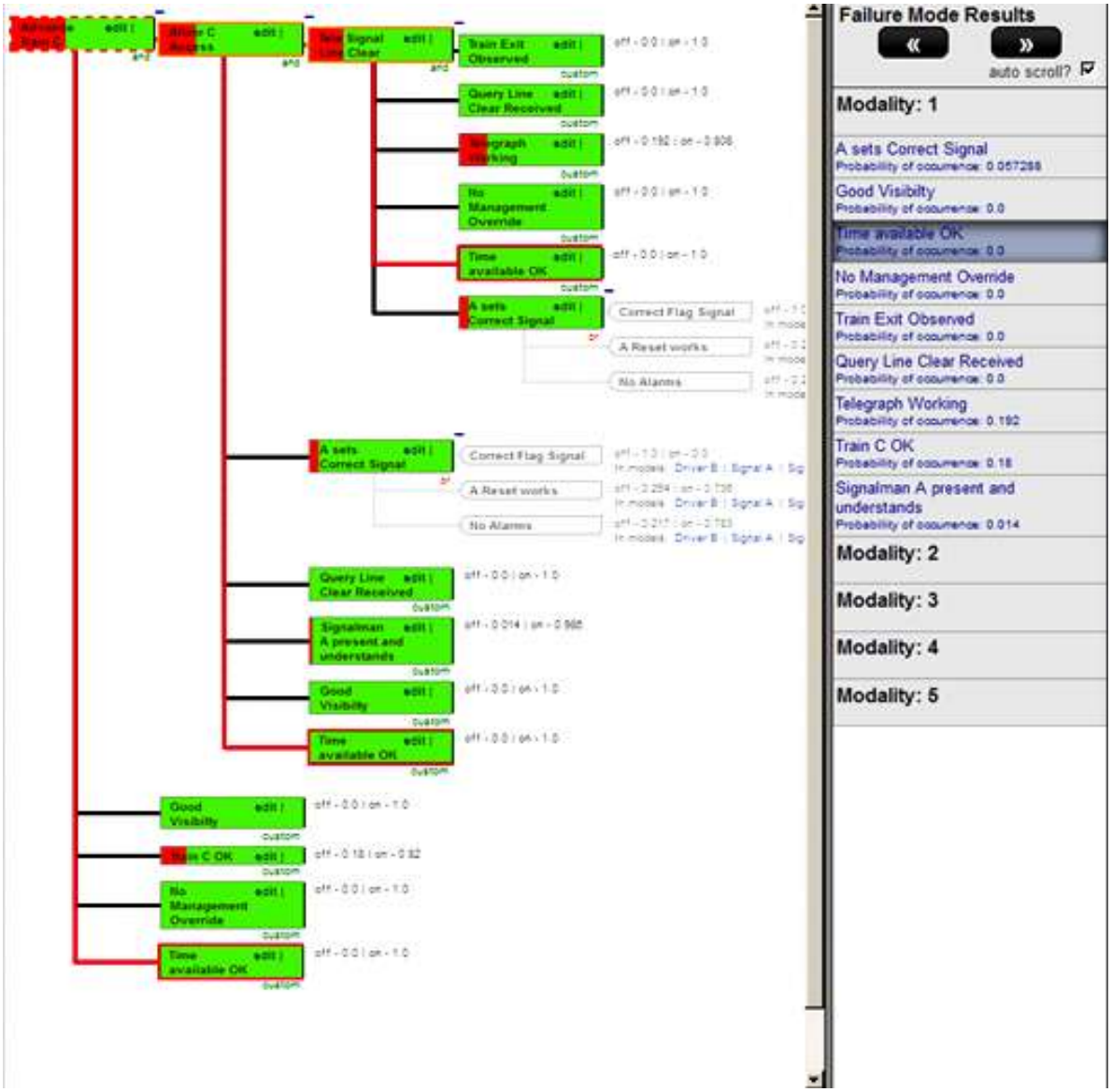
This indicates that with our models and reliability estimates, the system has a nominal probability of successful operation of some 61%.

Further the green bar indicates that even if we increase the mechanical reliability of the Telegraph to 100%, we can increase the overall success rate to about 80% (Pareto) at best.

Of more concern are the red bars, which indicate that on this model failure of any of 9 separate leaves can cause complete failure of the system. Most of these are “Human”, and illustrate well that assessing a system performance on purely mechanical reliability is at least incomplete?

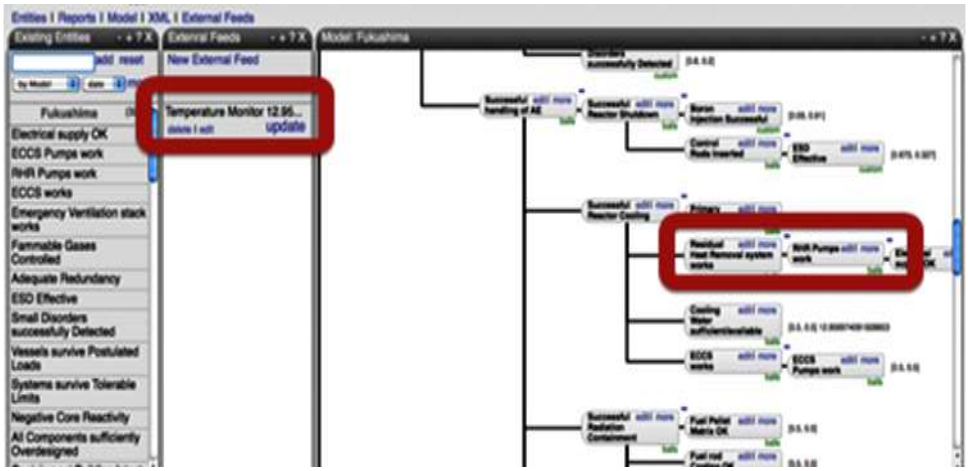
Also of interest is the failure mode analysis, which indicates that Time is involved in multiple critical dependencies


Sort Option
3 Point Sensitivity of Advance Train C to 9 leaves
Telegraph Working (0.7822)
Train C OK (0.751)
A sets Correct S... (0.6533)
Signalman A pres... (0.5248)
No Management Ove... (0.5159)
Good Visibility (0.5159)
Train Exit Observed (0.5159)
Query Line Clear ... (0.5159)
Time available OK (0.5159)
Leaves
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0.61585882
Sensitivity


Failure Mode Results
auto scroll?
Modality: 1
A sets Correct Signal
Probability of occurrence: 0.057286
Good Visibility
Probability of occurrence: 0.0
Time available OK
Probability of occurrence: 0.0
No Management Override
Probability of occurrence: 0.0
Train Exit Observed
Probability of occurrence: 0.0
Query Line Clear Received
Probability of occurrence: 0.0
Telegraph Working
Probability of occurrence: 0.192
Train C OK
Probability of occurrence: 0.18
Signalman A present and understands
Probability of occurrence: 0.014
Modality: 2
Modality: 3
Modality: 4
Modality: 5

CONCLUSION

We can now build a complete "System" containing all these interacting, interdependent functions. To this we can add spatial and environmental inputs again as "External Feeds" - dependencies common to many of the functions.



But the major attraction for the FRAM process is that now we have a permanent, accessible "model" to test interactions, variabilities, "Barriers", redesign "work arounds", or ensure responsible and aware Management of Change.

This illustrates the potential power and usefulness to be derived from the synergy possible from combining these two "Systemic" approaches and is surely worth pursuing further.

REFERENCES

- http://en.wikipedia.org/wiki/Clayton_Tunnel_rail_crash
- http://www.semgonline.com/misc/clayton-tun-acc.html
- ^ Parliament, House of Commons (1862). "Railways; Turnpike Trusts; Miscellaneous: Accounts and Papers". *Parliamentary Papers, Session 6 February - 7 August 1862* (HMSO) (Vol LIII): pp. 1793–1802.
- ^ "The Catastrophe On The London And Brighton Railway". *The Times*. 11 September 1861. p. 8.
- ^ "Death In The Tunnel". *The Times*. 25 August 1861. p. 10.
- ^ LTC Rolt, *Red For Danger*, p. 55
- L. T. C. Rolt, *Red for Danger: the classic history of British railway disasters*, Sutton Publishing (1998) ISBN 0-7509-2047-5
- Peter R Lewis, *Disaster on the Dee: Robert Stephenson's Nemesis of 1847*, Tempus 2007.
- Erik Hollnagel FRAM: The Functional Resonance Analysis Method - Modelling Complex Socio-Technical Systems, Ashgate Publishing Company, 2012
- *The Open Group Standard C 133* Dependency Modelling (O-DM) - Constructing a Data Model to Manage Risk and Build Trust between Inter-Dependent Enterprises 2012

Grateful Acknowledgements are due to, in particular –

Erik Hollnagel, David Porter, Jeremy Comer, Pete Burnap and John Gordon.