Clayton Tunnel – Can we shine any more light on it today?

Clayton Tunnel – Can we shine any more light on it today?

SAFETY HUMAN PERFORMANCE SYSTEM
"FROM THEORY TO PRACTICE"
Lisbon 24th & 26th September 2014

Eurocontrol Network Manager
NMD/NOM/SAF
ESP+ Programme
David Slater

©Cambrensis 2014

Clayton Tunnel 1861

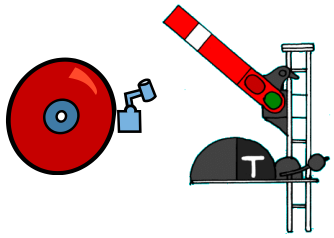
A high-risk environment requiring state-of-the-art protection to keep passengers safe

Only ONE train in either direction when inside the tunnel

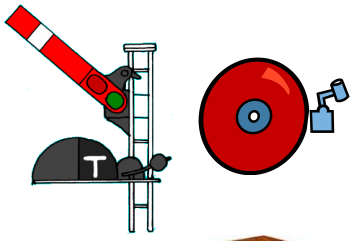
State-of-the-art protection

South

North

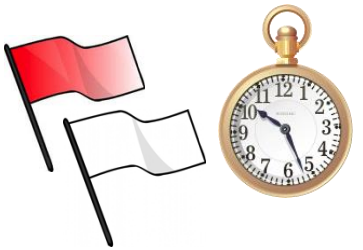


Tunnel



"train_in"
"train_out"
"is_train_out?"

"train_in"
"train_out"
"is_train_out?"

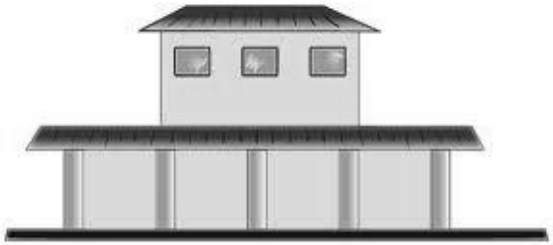


Multiple protective layers
Redundant components
Defined protocol
State-of-the-art technology
What could possibly go wrong?

Telegraphic protocol

- The-needle telegraph allows three signals:
  - “train_in”
  - “train_out”
  - (“is_train_out?”)
- Process:
  - train passes green signal
  - train enters tunnel
  - signal trips to red
  - signalman A telegraphs “train_in”
  - train traverses tunnel…
  - …train exits tunnel
  - signalman B telegraphs “train_out”
  - signalman A resets signal to green

Brighton station, 25 August 1861, 08:28



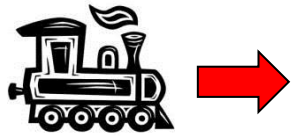
Assistant Station Master Legg

Driver Gregory

Brighton Parliamentary

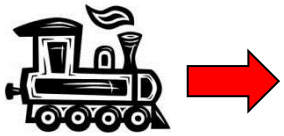
08:35 (08:30)

Driver Scott



Brighton Excursion

08:31 (08:15)

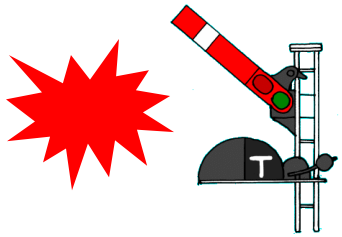


Portsmouth Excursion

08:28 (08:05)

Disaster strikes

South **North**



Tunnel

Portsmouth Excursion

25 – 30 mph

Brighton 5 miles

~ 1 Mile

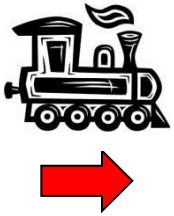
Killick **Brown**

Disaster strikes

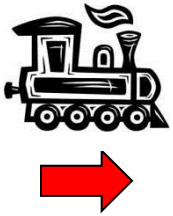
South **North**

Tunnel

Scott



Killick



Portsmouth Excursion

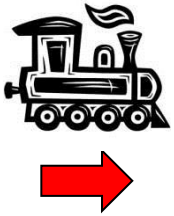
Disaster strikes

South

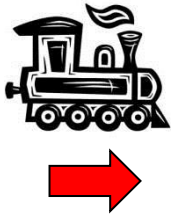
North

Tunnel

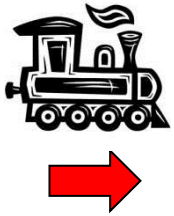
Gregory



Killick



Scott



Portsmouth
Excursion

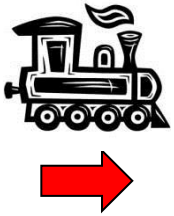
Disaster strikes

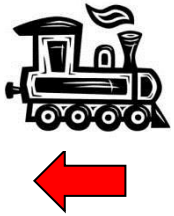
South

North

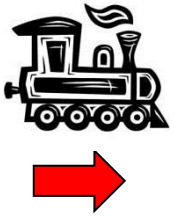
Tunnel

Gregory





Scott



is_train_out?

is_train_out?

train_out

train_out

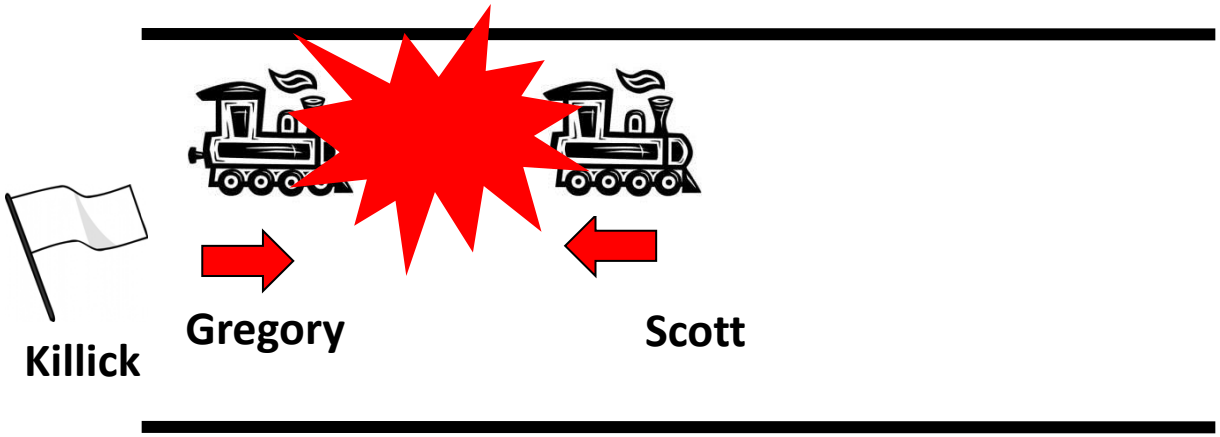
Killick

Brown

Disaster strikes

South **North**

Tunnel



23 killed, 176 seriously injured

Normal Cycle "As imagined"

Trains Dispatched
A. 8:05,
B. 8:15 and
C. 8:30

Semaphore at STOP

Train A approaches (T Minutes)

Signalman A telegraphs
"is Train out?"

Signalman B telegraphs "Train out"

Signalman A sets Semaphore at GO

Train Passes Semaphore at GO

Train A enters tunnel
(T + 1 minute)

Semaphore resets to STOP

Train B approaches (T+15 minutes).
Signalman A Telegraphs "Is Train in"
Signalman A telegraphs "Train out?"

Train A exits the Tunnel (T + 4 minutes)

Signalman B telegraphs "Train out"
(T + 4minutes)

Signalman A sets Semaphore at GO
(T + 4minutes)

Train B enters Tunnel (T + 16 minutes) Semaphore resets to STOP
Signalman A telegraphs "Is Train out?"
Train B exits Tunnel (T + 20 minutes)
Signalman B telegraphs "Train out"

Train C approaches (T + 30 minutes)
Signalman A sets Semaphore at GO
Train C enters Tunnel
(T + 30 minutes)

Train C exits Tunnel (T + 34minutes)

What was going on in the various parts of the system?

©Cambrensis 2014

Normal Cycle "As imagined"	*Deviation "As imagined"*
Trains Dispatched A. 8:05, B. 8:15 and C. 8:30	Trains Dispatched A. 8.28 (+23minutes), B. 8:31 (+16 minutes), C. 8:35 (+ 5 minutes)
Semaphore at STOP	**Semaphore at STOP**
Train A approaches (T Minutes)	**Train A approaches (T Minutes)**
Signalman A telegraphs "is Train out?"	**Signalman A telegraphs "is Train out?"**
Signalman B telegraphs "Train out"	**Signalman B telegraphs "Train out"**
Signalman A sets Semaphore at GO	**Signalman A sets Semaphore at GO**
Train Passes Semaphore at GO	**Train Passes Semaphore at GO**
Train A enters tunnel (T + 1 minute)	**Train A enters tunnel (T + 1 minute)**
Semaphore resets to STOP	***Semaphore sticks at GO*** ***Alarm sounds***
Train B approaches (T+15 minutes). **Signalman A Telegraphs "Is Train in"** **Signalman A** telegraphs "Train out?"	**Train B approaches** (T+ 3minutes) **Signalman A** flags STOP Signalman A telegraphs "Train out?"
Train A exits the Tunnel (T + 4 minutes)	**Train A exits the Tunnel (T + 4 minutes)**
Signalman B telegraphs "Train out" (T + 4minutes)	**Signalman B telegraphs "Train out"** (T + 4minutes)
Signalman A sets Semaphore at GO (T + 4minutes)	**Signalman A resets Semaphore at GO** **or** Signalman A flags GO (T + 4minutes) Train B passes Semaphore and Flags at GO
Train B enters Tunnel (T + 16 minutes) Semaphore resets to STOP **Signalman A** telegraphs "Is Train out?" **Train B exits Tunnel (T + 20 minutes)** **Signalman B telegraphs "Train out"**	**Train B enters Tunnel (T + 16 minutes)** **Signalman A** telegraphs "Is Train out?" **Train B exits Tunnel (T + 20 minutes)** **Signalman B telegraphs "Train out"**
Train C approaches (T + 30 minutes) **Signalman A sets Semaphore at GO** **Train C enters Tunnel** (T + 30 minutes)	**Train C approaches (T + 30 minutes)** Signalman A flags GO (T + 30minutes) **Train C enters Tunnel** (T + 30 minutes)
Train C exits Tunnel (T + 34minutes)	**Train C exits Tunnel** (T + 34minutes)

What was going on in the various parts of the system?

©Cambrensis 2014

Normal Cycle "As imagined"	*Deviation "As imagined"*	*Deviation with Signalman Function "As is"*
Trains Dispatched **A. 8:05,** **B. 8:15 and** **C. 8:30**	Trains Dispatched A. 8.28 (+23minutes), B. 8:31 (+16 minutes), C. 8:35 (+ 5 minutes)	Trains Dispatched A. 8.28 (+23minutes), B. 8:31 (+16 minutes), C. 8:35 (+ 5 minutes)
Semaphore at STOP	**Semaphore at STOP**	**Semaphore at STOP**
Train A approaches(T Minutes)	**Train A approaches(T Minutes)**	**Train A approaches(T Minutes)**
Signalman A telegraphs "is Train out?"	**Signalman A telegraphs "is Train out?"**	**Signalman A telegraphs "is Train out?"**
Signalman B telegraphs "Train out"	**Signalman B telegraphs "Train out"**	**Signalman B telegraphs "Train out"**
Signalman A sets Semaphore at GO	**Signalman A sets Semaphore at GO**	**Signalman A sets Semaphore at GO**
Train Passes Semaphore at GO	**Train Passes Semaphore at GO**	**Train Passes Semaphore at GO**
Train A enters tunnel **(T + 1 minute)**	**Train A enters tunnel** **(T + 1 minute)**	**Train A enters tunnel** **(T + 1 minute)**
Semaphore resets to STOP	***Semaphore sticks at GO*** ***Alarm sounds***	***Semaphore sticks at GO*** ***Alarm Sounds***
Train B approaches (T+15 minutes). **Signalman A Telegraphs "Is Train in"** **Signalman A** telegraphs "Train out?"	**Train B approaches** (T+ 3minutes) **Signalman A** flags STOP Signalman A telegraphs "Train out?"	**Train B approaches** (T + 3 minutes) **Train B passes Semaphore at "GO"** **Signalman A prepares to use Flags** **Train B enters Tunnel** (T + 3 .5 minutes)
Train A exits the Tunnel(T + 4 minutes)	**Train A exits the Tunnel(T + 4 minutes)**	**Train A exits the Tunnel (T + 4 minutes)**
Signalman B telegraphs "Train out" (T + 4minutes)	**Signalman B telegraphs "Train out"** (T + 4minutes)	**Signalman B** telegraphs "Train out" (T + 4minutes)
Signalman A sets Semaphore at GO (T + 4minutes)	**Signalman A resets Semaphore at GO or** Signalman A flags GO (T + 4minutes) Train B passes Semaphore and Flags at GO	**Signalman A** Flags STOP (T + 4 minutes)
Train B enters Tunnel (T + 16 minutes) Semaphore resets to STOP **Signalman A** telegraphs "Is Train out?" **Train B exits Tunnel (T + 20 minutes)** **Signalman B telegraphs "Train out"**	**Train B enters Tunnel (T + 16 minutes)** **Signalman A** telegraphs "Is Train out?" **Train B exits Tunnel (T + 20 minutes)** **Signalman B telegraphs "Train out"**	**Signalman A** telegraphs" Is Train out?" (T + 5minutes) **Train B exits Tunnel** (T + 7minutes) **Signalman B telegraphs "Train out"**
Train C approaches (T + 30 minutes) **Signalman A sets Semaphore at GO** **Train C enters Tunnel** (T + 30 minutes)	**Train C approaches (T + 30 minutes)** Signalman A flags GO (T + 30minutes) **Train C enters Tunnel** (T + 30 minutes)	**Train C approaches (T + 7 minutes)** **Signalman A** flags GO (T + 7 minutes) **Train C enters Tunnel** (T + 7 minutes)
Train C exits Tunnel (T + 34minutes)	**Train C exits Tunnel** (T + 34minutes)	**Train C exits Tunnel** (T + 11 minutes)

What was going on in the various parts of the system?

©Cambrensis 2014

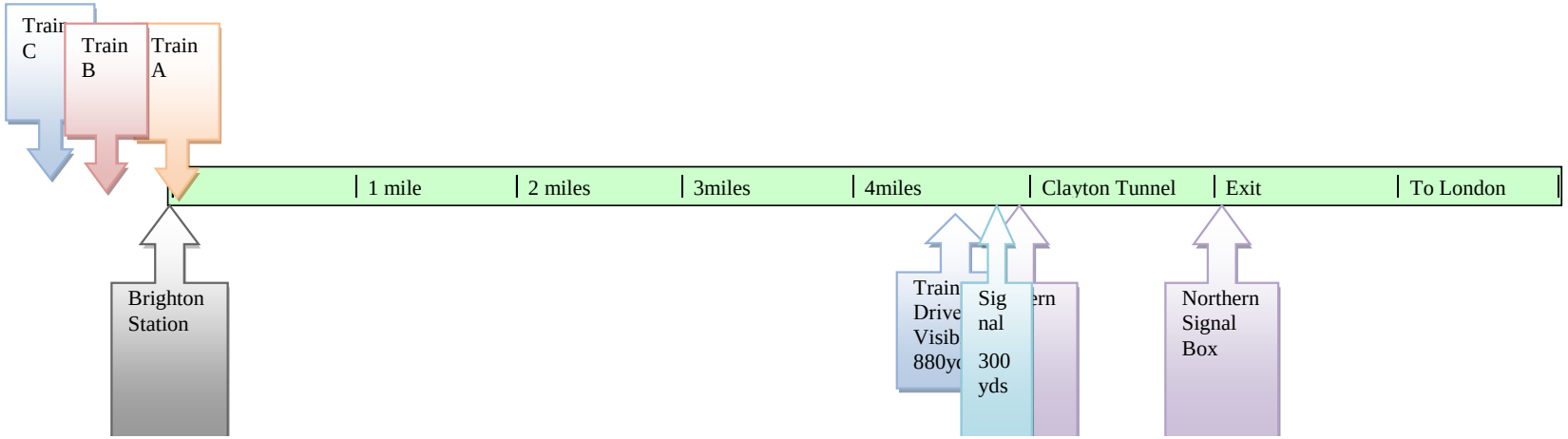
Normal Cycle "As imagined"	*Deviation "As imagined"*	*Deviation with Signalman Function "As is"*	*Deviation with both signalman and Train Driver Function "As is"*
Trains Dispatched A. 8:05, B. 8:15 and C. 8:30	Trains Dispatched A. 8.28 (+23minutes), B. 8:31 (+16 minutes), C. 8:35 (+ 5 minutes)	Trains Dispatched A. 8.28 (+23minutes), B. 8:31 (+16 minutes), C. 8:35 (+ 5 minutes)	Trains Dispatched A. 8.28 (+23minutes), B. 8:31 (+16 minutes), C. 8:35 (+ 5 minutes)
Semaphore at STOP	**Semaphore at STOP**	**Semaphore at STOP**	**Semaphore at STOP**
Train A approaches (T Minutes)	**Train A approaches (T Minutes)**	**Train A approaches (T Minutes)**	**Train A approaches (T Minutes)**
Signalman A telegraphs "is Train out?"	**Signalman A telegraphs "is Train out?"**	**Signalman A telegraphs "is Train out?"**	**Signalman A telegraphs "is Train out?"**
Signalman B telegraphs "Train out"	**Signalman B telegraphs "Train out"**	**Signalman B telegraphs "Train out"**	**Signalman B telegraphs "Train out"**
Signalman A sets Semaphore at GO	**Signalman A sets Semaphore at GO**	**Signalman A sets Semaphore at GO**	**Signalman A sets Semaphore at GO**
Train Passes Semaphore at GO	**Train Passes Semaphore at GO**	**Train Passes Semaphore at GO**	**Train Passes Semaphore at GO**
Train A enters tunnel (T + 1 minute)	**Train A enters tunnel (T + 1 minute)**	**Train A enters tunnel (T + 1 minute)**	**Train A enters tunnel (T + 1 minute)**
Semaphore resets to STOP	***Semaphore sticks at GO Alarm sounds***	***Semaphore sticks at GO Alarm Sounds***	***Semaphore sticks at GO Alarm Sounds***
Train B approaches (T+15 minutes). Signalman A Telegraphs "Is Train in" Signalman A telegraphs "Train out?"	**Train B approaches** (T+ 3minutes) **Signalman A** flags STOP Signalman A telegraphs "Train out?"	**Train B approaches** (T + 3 minutes) **Train B passes Semaphore at "GO" Signalman A prepares to use Flags Train B enters Tunnel** (T + 3 .5 minutes)	Train B approaches(T + 3 minutes) **Train B passes Semaphore at "GO" Signalman A prepares to use Flags Train B enters Tunnel** (T+ 3 .5 minutes)
Train A exits the Tunnel (T + 4 minutes)	**Train A exits the Tunnel (T + 4 minutes)**	**Train A exits the Tunnel (T + 4 minutes)**	**Train A exits the Tunnel (T + 4 minutes)**
Signalman B telegraphs "Train out" (T + 4minutes)	**Signalman B telegraphs "Train out"** (T + 4minutes)	**Signalman B** telegraphs "Train out" (T + 4minutes)	**Signalman B telegraphs "Train out"** (T + 4minutes)
Signalman A sets Semaphore at GO (T + 4minutes)	**Signalman A resets Semaphore at GO or** Signalman A flags GO (T + 4minutes) Train B passes Semaphore and Flags at GO	**Signalman A** Flags STOP (T + 4 minutes)	**Signalman A** Flags STOP (T + 4minutes)
Train B enters Tunnel (T + 16 minutes) Semaphore resets to STOP Signalman A telegraphs "Is Train out?" **Train B exits Tunnel (T + 20 minutes) Signalman B telegraphs "Train out"**	**Train B enters Tunnel (T + 16 minutes) Signalman A** telegraphs "Is Train out?" **Train B exits Tunnel (T + 20 minutes) Signalman B telegraphs "Train out"**	**Signalman A** telegraphs" Is Train out?" (T + 5minutes) **Train B exits Tunnel** (T + 7minutes) **Signalman B telegraphs "Train out"**	***Train B stops in Tunnel*** (T + 5 minutes) ***Train B reverses*** (T + 6 minutes)
Train C approaches (T + 30 minutes) Signalman A sets Semaphore at GO Train C enters Tunnel (T + 30 minutes)	**Train C approaches (T + 30 minutes)** Signalman A flags GO (T + 30minutes) **Train C enters Tunnel** (T + 30 minutes)	**Train C approaches (T + 7 minutes) Signalman A** flags GO (T + 7 minutes) **Train C enters Tunnel** (T + 7 minutes)	**Train C approaches (T + 7 minutes) Signalman A** Flags GO (T + 7 minutes) **Train C enters Tunnel** (T + 7 minutes)
Train C exits Tunnel (T + 34minutes)	**Train C exits Tunnel** (T + 34minutes)	**Train C exits Tunnel** (T + 11 minutes)	***Trains C and B collide*** (T + 8 minutes)

What was going on in the various parts of the system?

©Cambrensis 2014

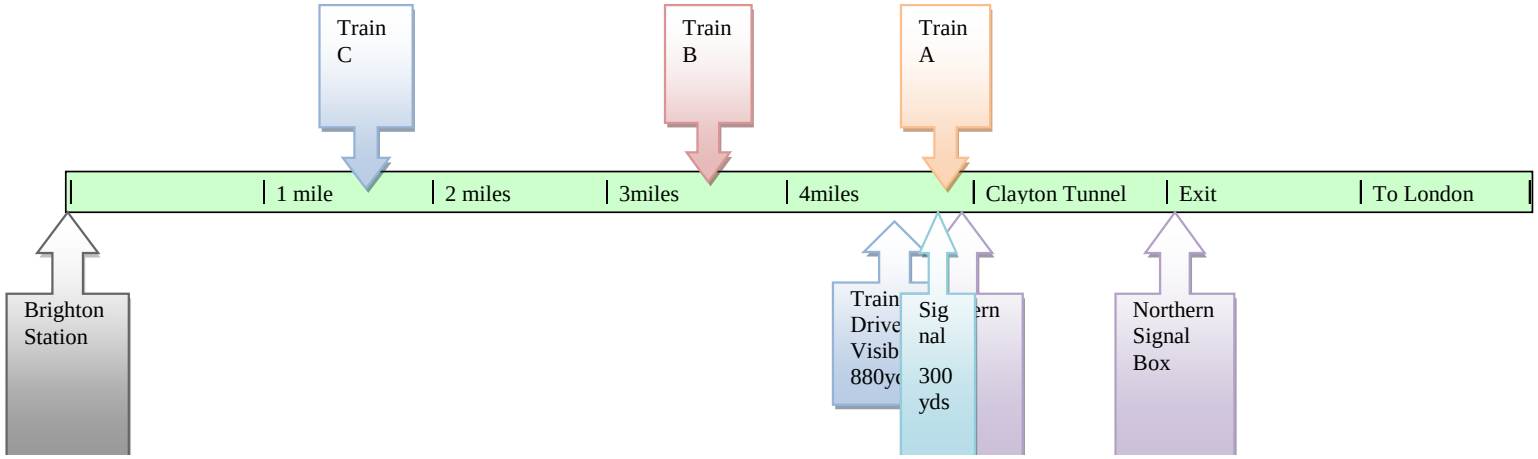
Or in ATM Parlance?

Separation Distances at 8:28



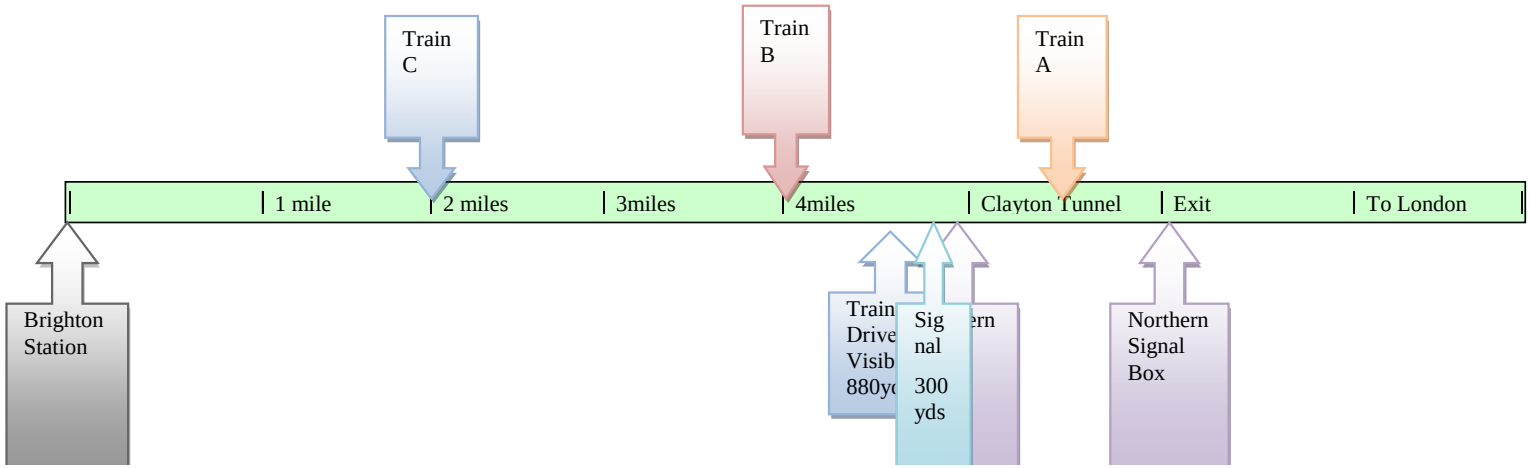
©Cambrensis 2014

Separation Distances at 8:38



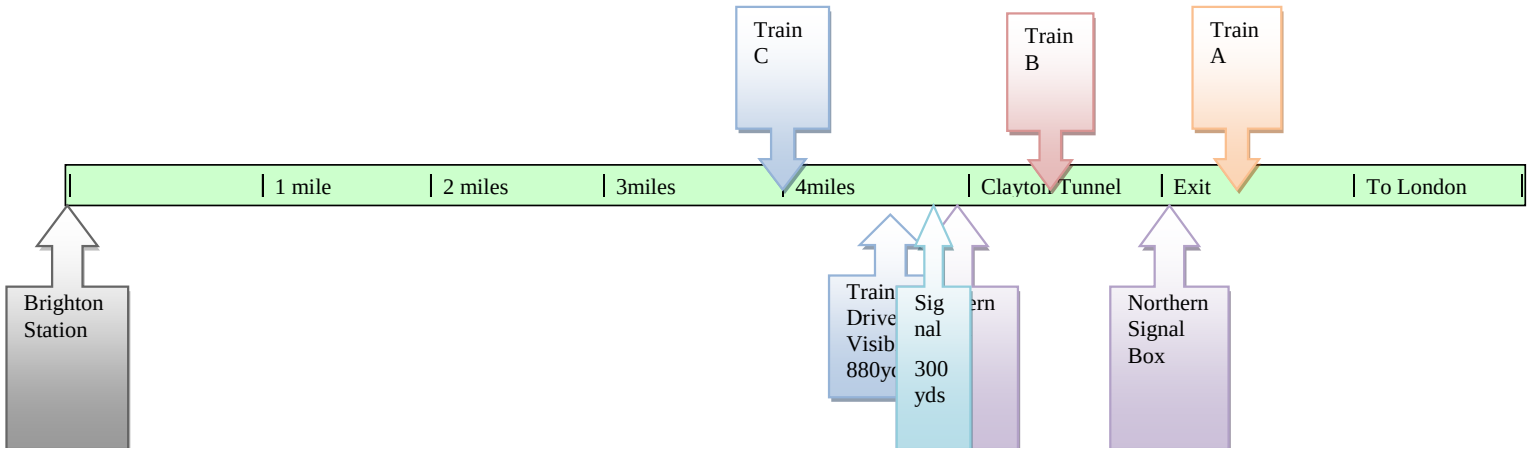
©Cambrensis 2014

Separation Distances at 8:40



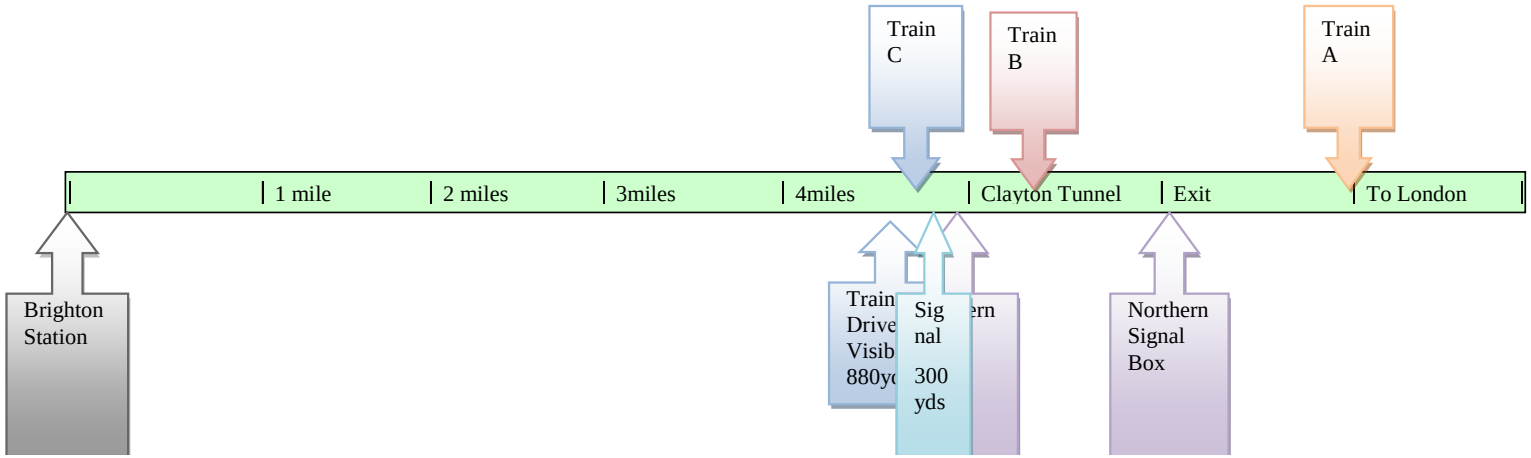
©Cambrensis 2014

Separation Distances at 8:44



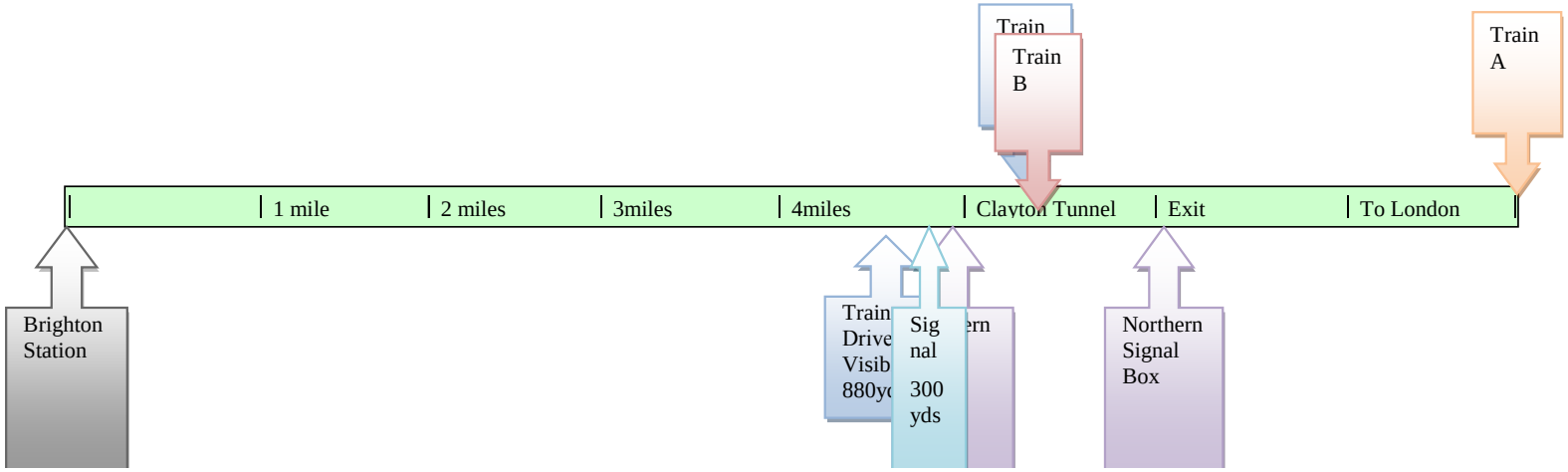
©Cambrensis 2014

Separation Distances at 8:45



©Cambrensis 2014

Separation Distances at 8:46



©Cambrensis 2014

WHY?

- Trains dispatched too closely (TIME, PROCEDURES, TRAINING))
- Driver B enters tunnel because he sees Flag too late. (TIME)
- Driver B stops in Tunnel unsure of situation. (PROCEDURES, COMPLEXITY)
- Signalman B sees “wrong” Train leave the tunnel (TIME, COMPLEXITY, COMMUNICATION)
- Driver B reverses to clarify red flag (PROCEDURES, TRAINING)
- Signalman A white flags Driver C through (COMMUNICATION)
- Collision (“RESONANCE” (or negative synergy/ exponential error?-) TIME/PROCEDURES, COMMUNICATION)

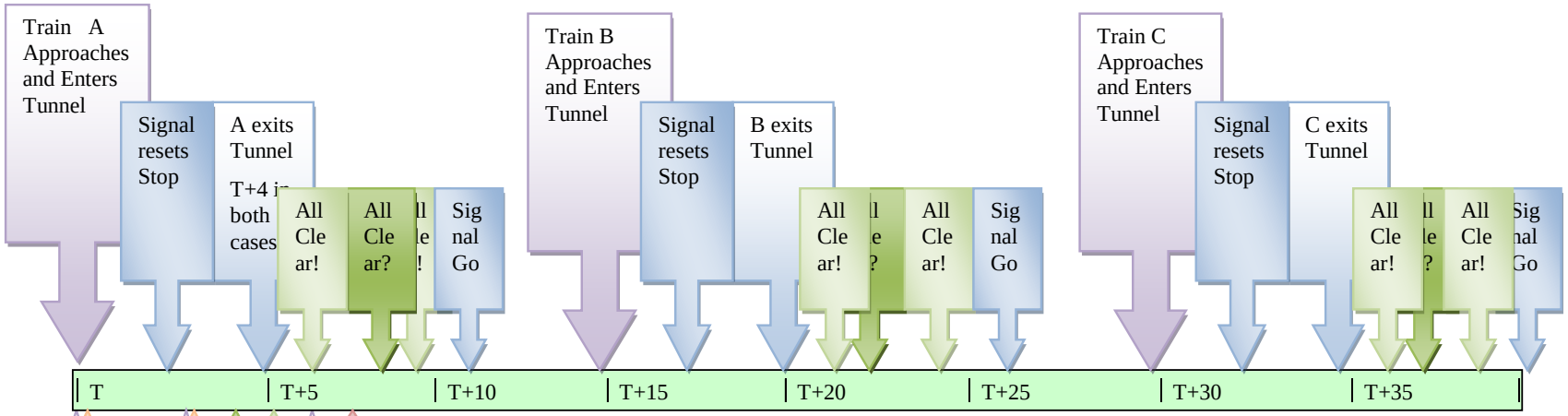
©Cambrensis 2014

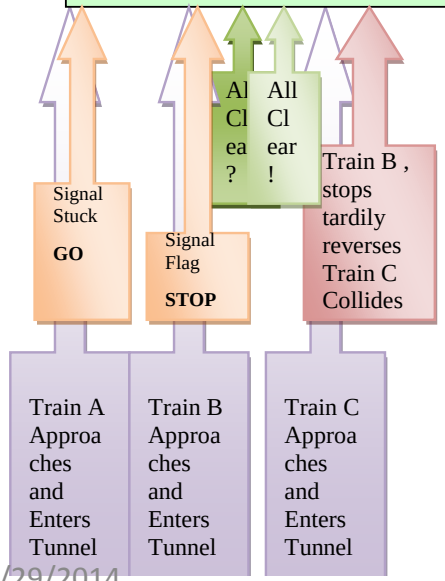
"As Imagined"

Clayton Tunnel Entrance control System

Incident Timeline

- An orderly "sequence" of actions, with "fail safe" handovers?





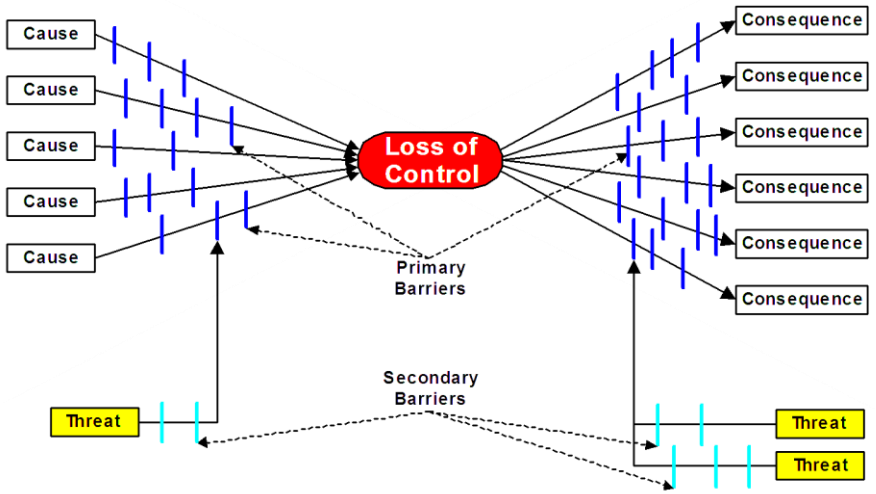
"As Was"

- It was not a simple "linear" piece of "elastic"
- that you could stretch or compress at will!
- and expect everything to "Stay Put", or adapt,
- in the same Relative, Relational configurations!

©Cambrensis 2014

How do you pick this up? Current Methods?

- FMEA?
- Full PRA?
- Bow Ties and Barriers?
- LOPA, SIL?
- HAZOP?

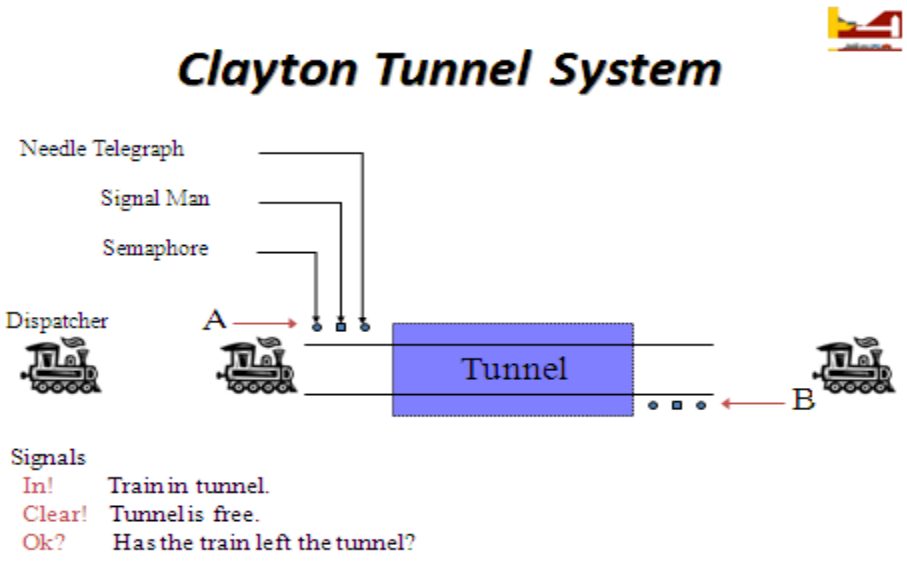


- All systematic, deterministic, component by component, in sequence, independent, As designed, "Linear" approaches.
- Quantitative answers misleading?

©Cambrensis 2014

Clayton System Integrity Level (Calculated?)

- Using a Layers of Protection Analysis (LOPA) approach, this gives us a perfectly acceptable System Integrity Level (SIL) which we can rely on to document the reliability of our design?
- Signal probability of Failure on Demand - (PFD) say $1x10^{-4}$?
- Signalman PFD – say $1x10^{-2}$?
- Telegraph PFD – say $1x10^{-4}$?
- SIL = $1x10^{-10}$? Safe as Houses!



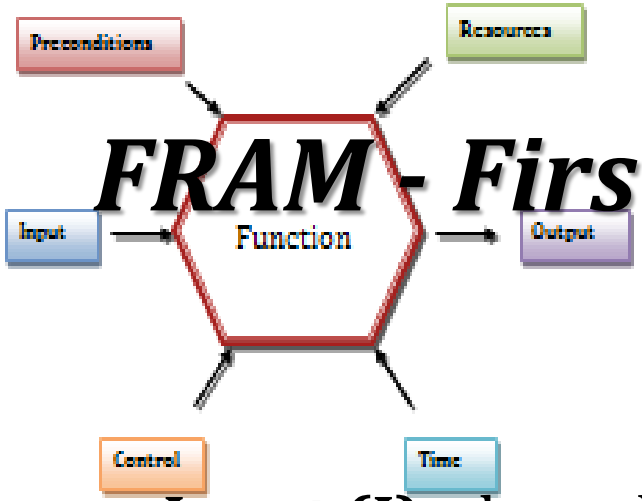
But it Happened – unlucky?

How <u>should</u> we pick this up?

- We need a non- linear, “system wide”, approach that can predict the often unexpected interactive effects of real life VARIABILITY.
- To pick up unintended RESONANCE between contributing (critical) functions in a system and link their DEPENDENCIES
- To “measure” the (relative) effectiveness of designed RESILIENCE and safeguards.
- A FRAM/BBN approach?

Because Interacting Functions can Vary and Resonate!

- As Hollnagel pointed out, simple linear deterministic models cannot cope with the actual tightly coupled and intractable functions in real systems.
- There is a need for inherently probabilistic models, which can capture not only **average** situations, but
- Also those which occur with very low frequency, but often then lead to disasters.
- Systems increase in complexity, increasingly dynamic.
- There is also a time dependence, (e.g. in the degradation or ageing processes of technological, human and management sub-systems).
- **Safety II and FRAM** are thus a necessary step in the evolution of Risk Methods to tackle **real systems** in **real applications**.
- ***(RESILIENCE - its going to happen – deal with it?)***



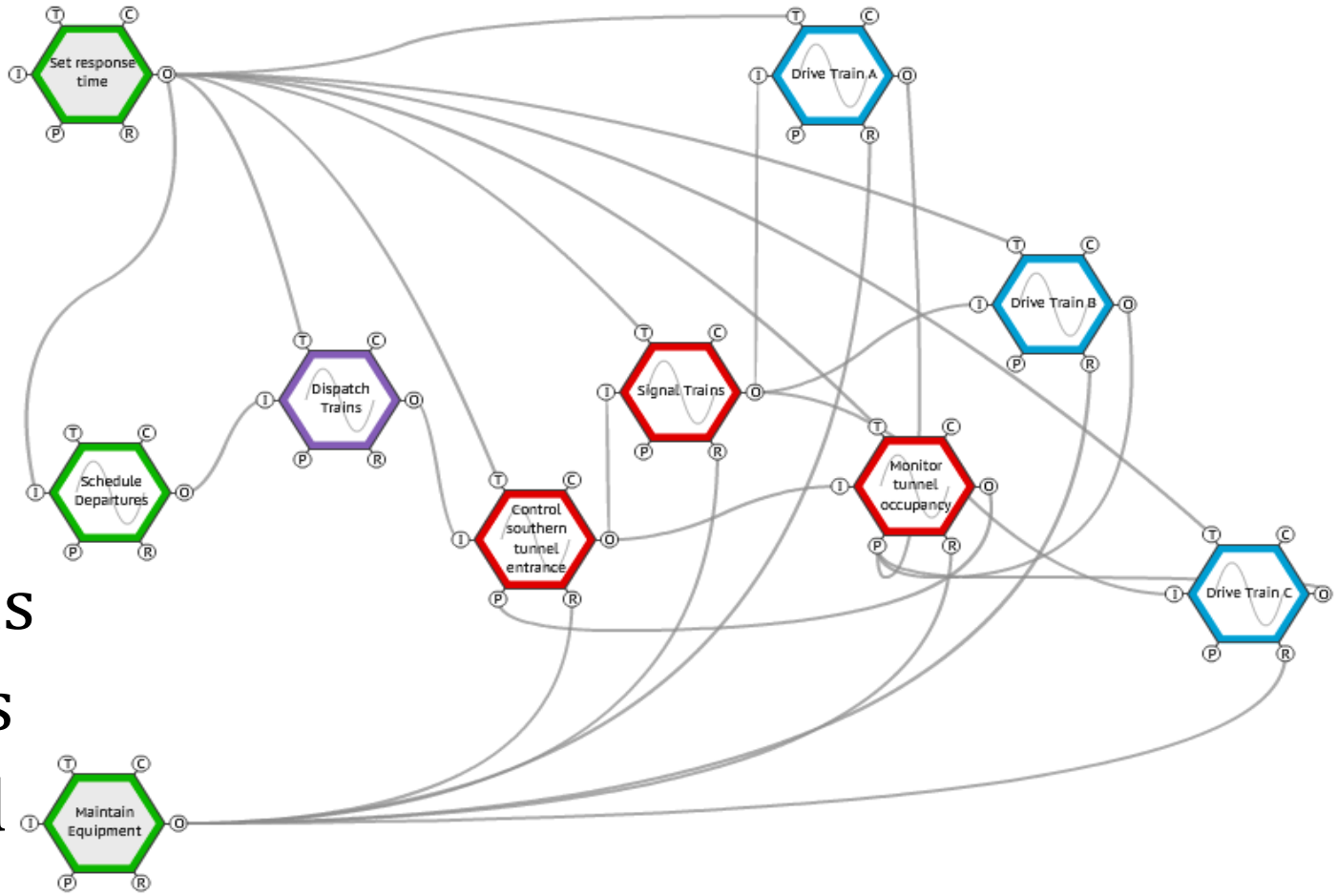
FRAM - First Define your Functions

- **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.

©Cambrensis 2014

E.g. Functions needed for Clayton Tunnel

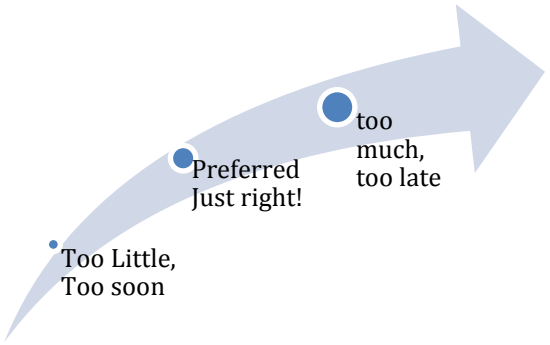
- Dispatch Trains
- Control Tunnel Entrance
- Monitor Tunnel Exit
- Signal Trains
- Drive Trains
- Background Functions

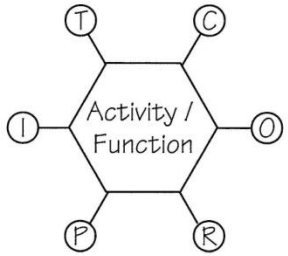


©Cambrensis 2014

Then Vary the Interaction Aspects?

- How?
- Luck of the draw, roll the dice?
- By inspection, Discussion





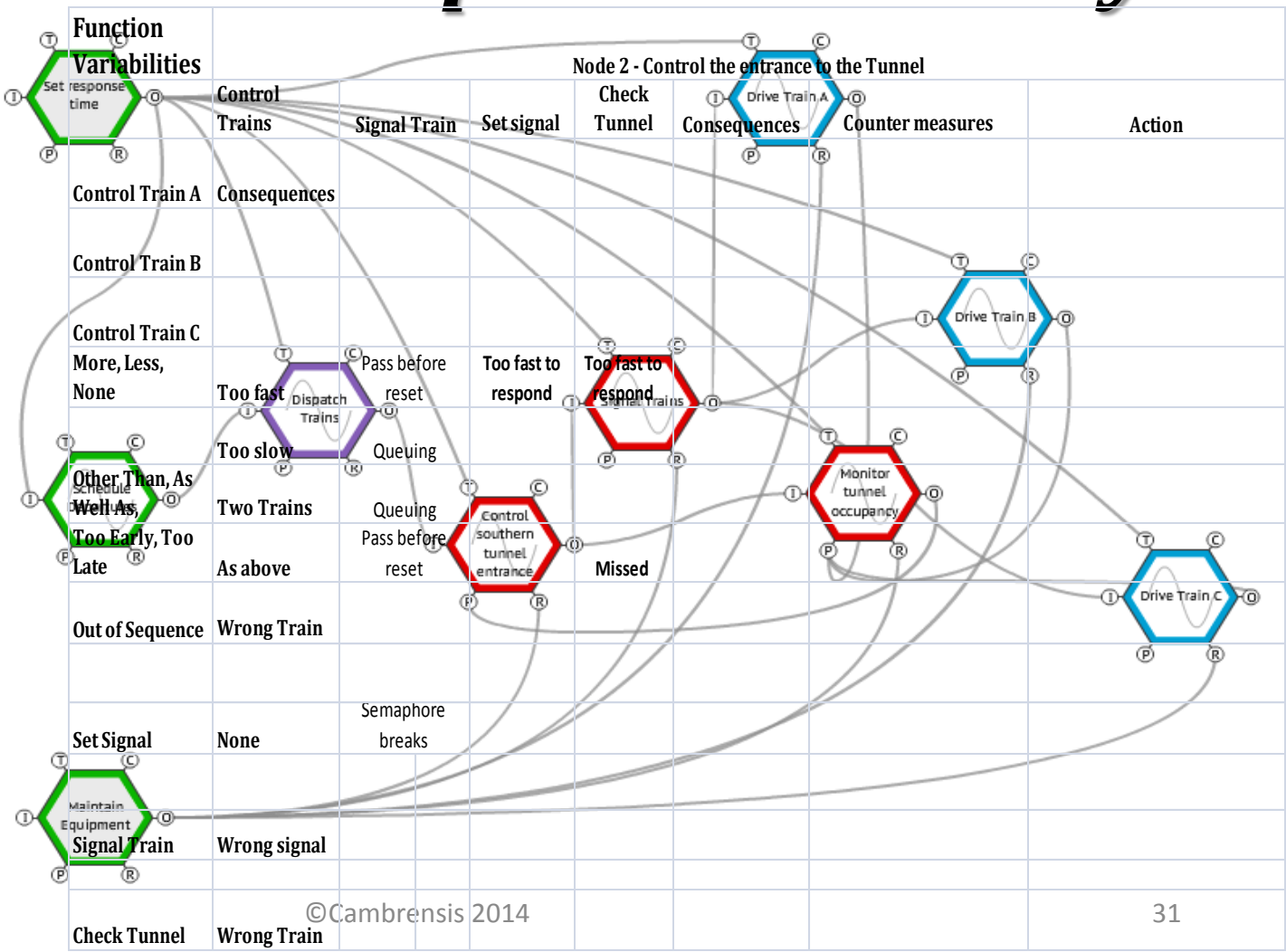
Speed	Too fast, too slow
Distance	Too far, too short
Sequence	Reversal, repetition, Commission, intrusion
Object	Wrong action, wrong object
Force	Too much, too little
Duration	Too long, too short
Direction	Wrong direction
Timing	Too early, too late, omission

- Or use HAZOP type guidewords?

©Cambrensis 2014

Use the HAZOP Guidewords to explore Variability?

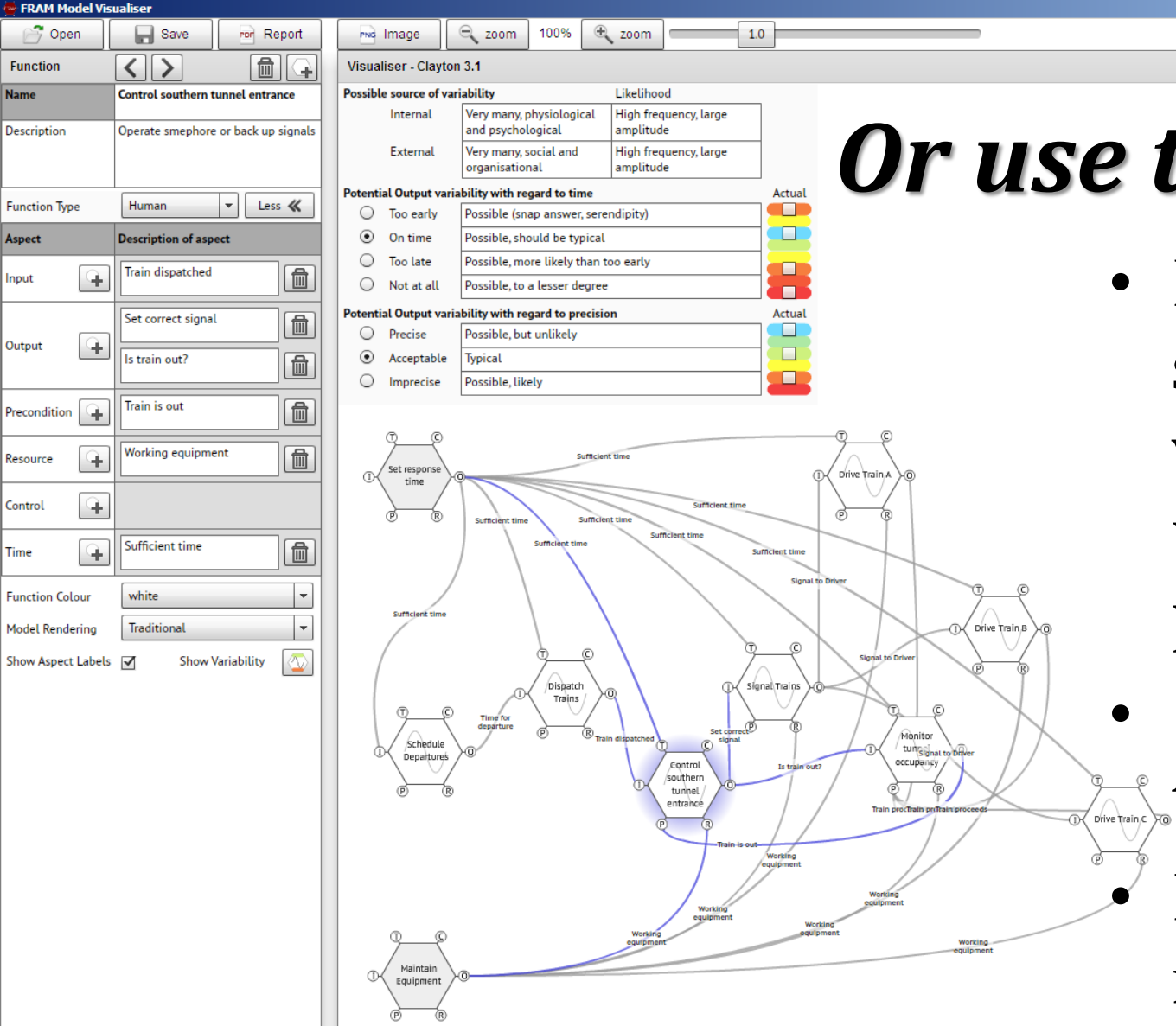
- Too Much?
- Too Little?
- Too Early?
- Too Late?



©Cambrensis 2014

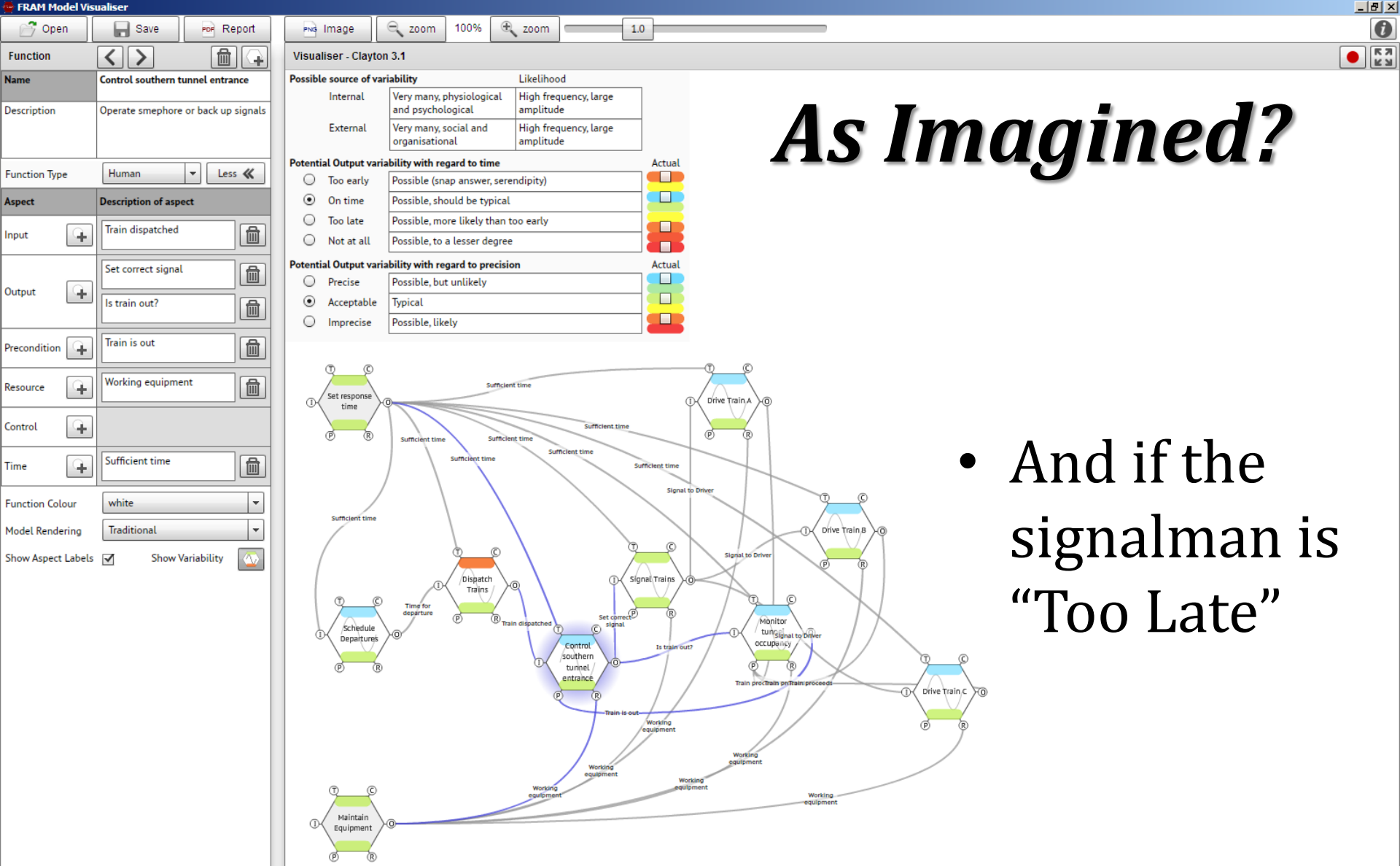
Or use the FMV*

- Here we can set estimated variabilities using the preset options,
- or set “Actual” to test What if.
- E.g. Best guess if signalman is “On Time”



©Cambrensis 2014

As Imagined?



- And if the signalman is "Too Late"

©Cambrensis 2014

FRAM Model Visualiser

Open | Save | Report | Image | zoom | 100% | zoom | 1.0

Function

Name	Control southern tunnel entrance
Description	Operate smephore or back up signals
Function Type	Human

Aspect	Description of aspect
Input	Train dispatched
Output	Set correct signal
	Is train out?
Precondition	Train is out
Resource	Working equipment
Control	
Time	Sufficient time

Function Colour: white

Model Rendering: Traditional

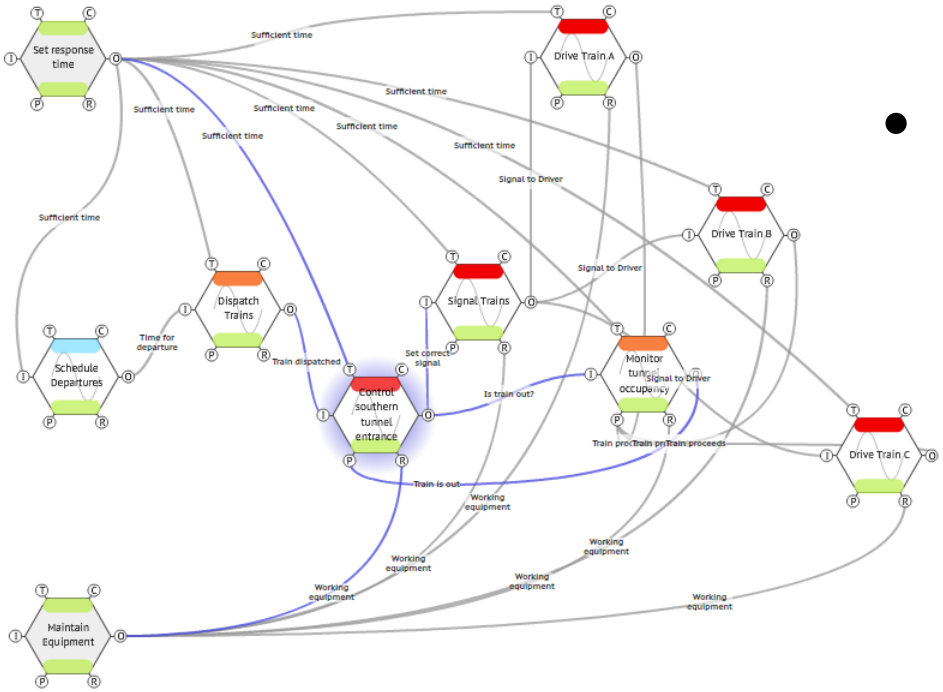
Show Aspect Labels ☑ Show Variability

Visualiser - Clayton 3.1

Possible source of variability		Likelihood
Internal	Very many, physiological and psychological	High frequency, large amplitude
External	Very many, social and organisational	High frequency, large amplitude

Potential Output variability with regard to time		Actual
○ Too early	Possible (snap answer, serendipity)	
○ On time	Possible, should be typical	
◉ Too late	Possible, more likely than too early	
○ Not at all	Possible, to a lesser degree	

Potential Output variability with regard to precision		Actual
○ Precise	Possible, but unlikely	
◉ Acceptable	Typical	
○ Imprecise	Possible, likely	



As Was!

- We are now clearly outside "Acceptable Limits" of operation

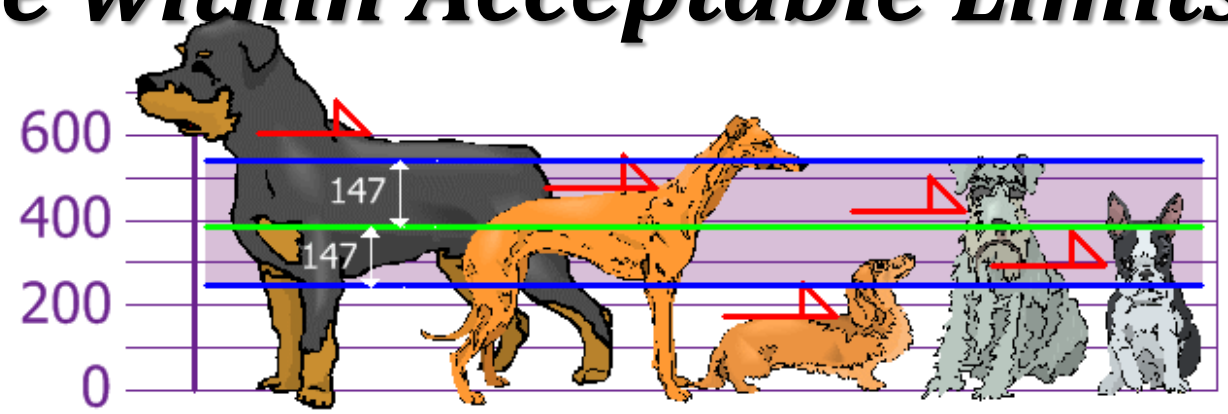
©Cambrensis 2014

Start | Sent Items - Microsoft O... | FRAM Model Visualiser | Document1 - Microsoft ... | Microsoft PowerPoint - [...] | 09:53

What were the Acceptable Limits?

- The Timeline shows the "As Imagined" Cycle taking 10 minutes
- This probably allowed for 3 – 5 minutes for the reset cycle.
- The reported time separation at dispatch was 3 minutes, close to the limit
- The "As Was" time available for the response to the signal reset failure was probably of the order of a minute (Half a mile at 30mph)
- Insufficient time for (tired) signalman to respond.
- The FRAM analysis predicts system failure for Signal "Too late"

Then what is the Probability that we are within Acceptable Limits?

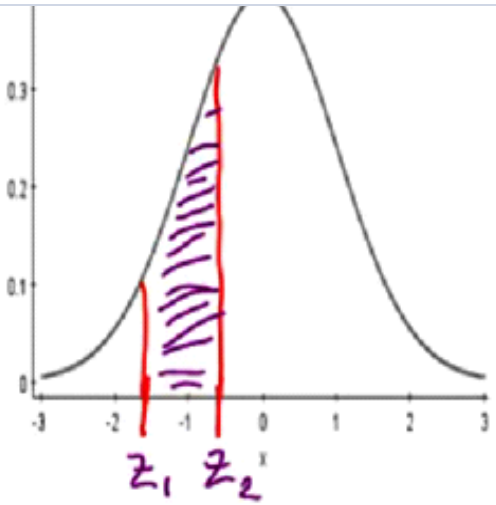


Rand Var X	500
μ Mean	420
σ Std Dev	240
Z	0.333333333

$$z = \frac{X - \mu}{\sigma}$$

0.226627352	0.226627352

Acceptable	
Z1	-0.75
X1	240
Z2	0.75
X2	600
Mean	420
Std Dev	240



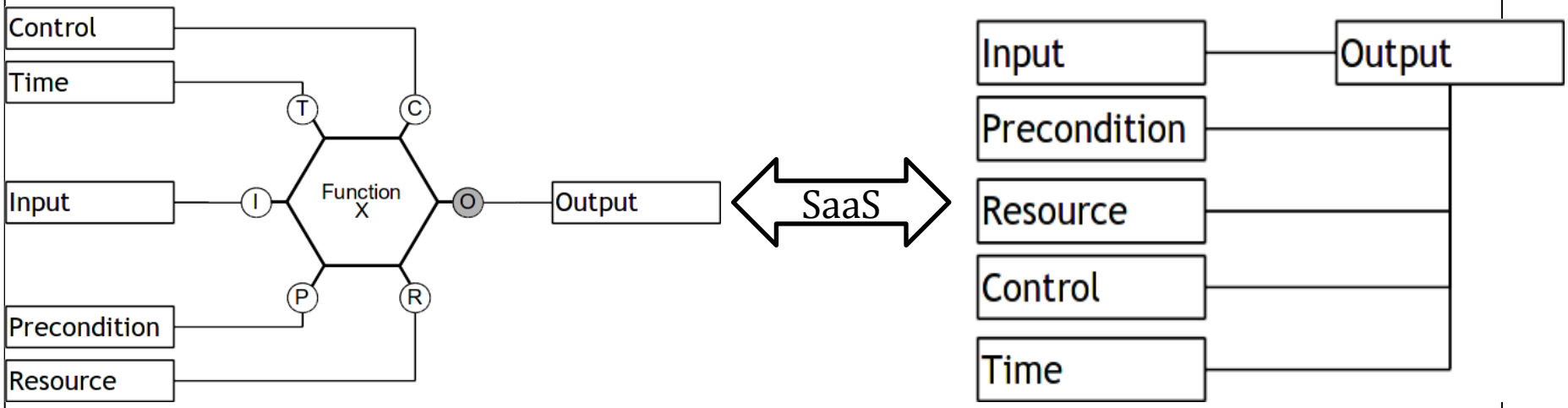
Type; Standard Normal Curve

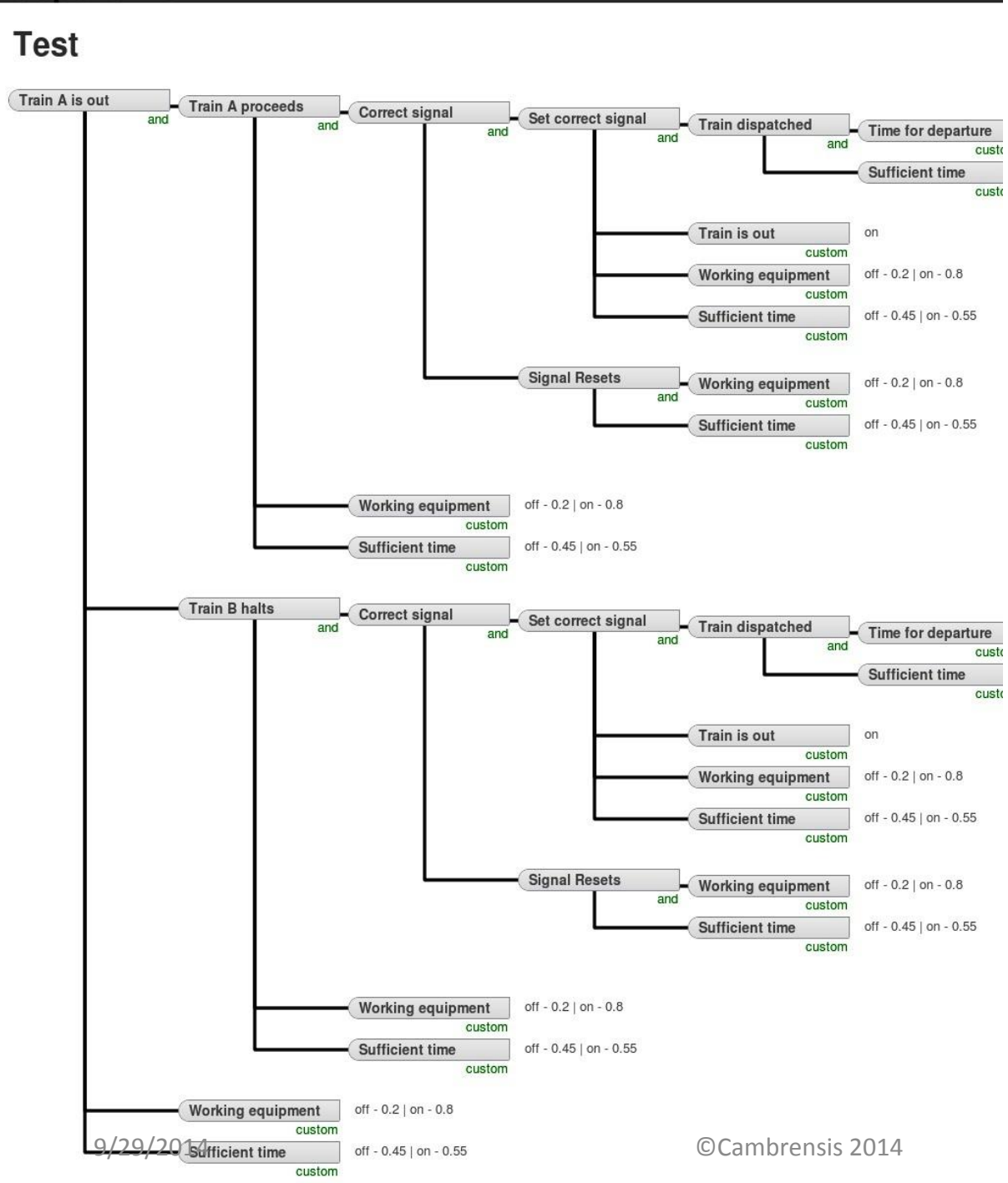
Mean	
Std Dev	

PA	0.546745295

How do we use this probability?

From (FRAM) Function to Bayesian Net (BBN)





Calculate Probabilities?

This version of the FMV now allows me to upload and present this FRAM as a Dependency Model

But interestingly is only asking me for the probabilities of two background Functions

- Speed of response and

- Maintenance effectiveness

©Cambrensis 2014

Probability of "Acceptability" of Background Outputs

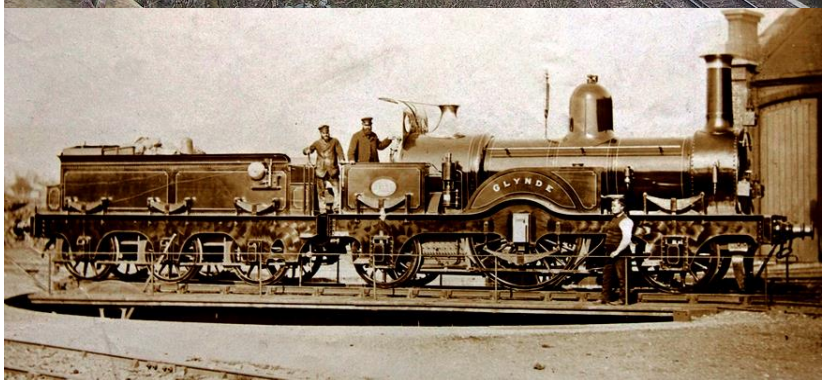
- **Speed of response -** take CREAM* approach from the Swiss Tunnel Risk Study the tunnel operator's response time affects two particular input variables of the model.

The first one is the

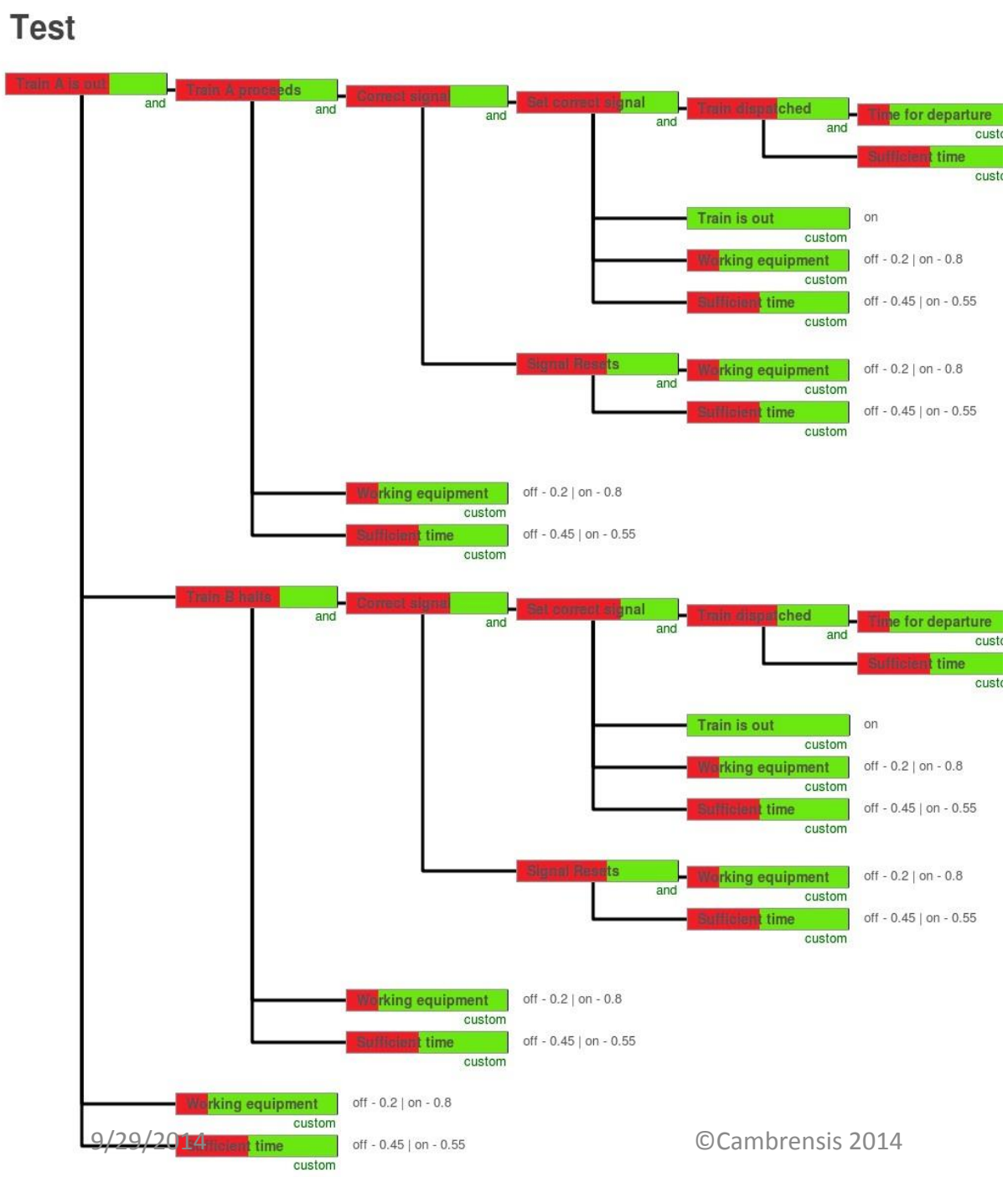
- 'time taken to activate the emergency ventilation' and the other one is
- the 'time delay to stop approaching traffic'.

  A tunnel operator with "inappropriate MMI", "Appropriate Procedures" and "inadequate training" will react in the range of 240s to 600s (expected value 420s – 7 minutes)

- **Maintenance** - assume 80/20 Pareto?



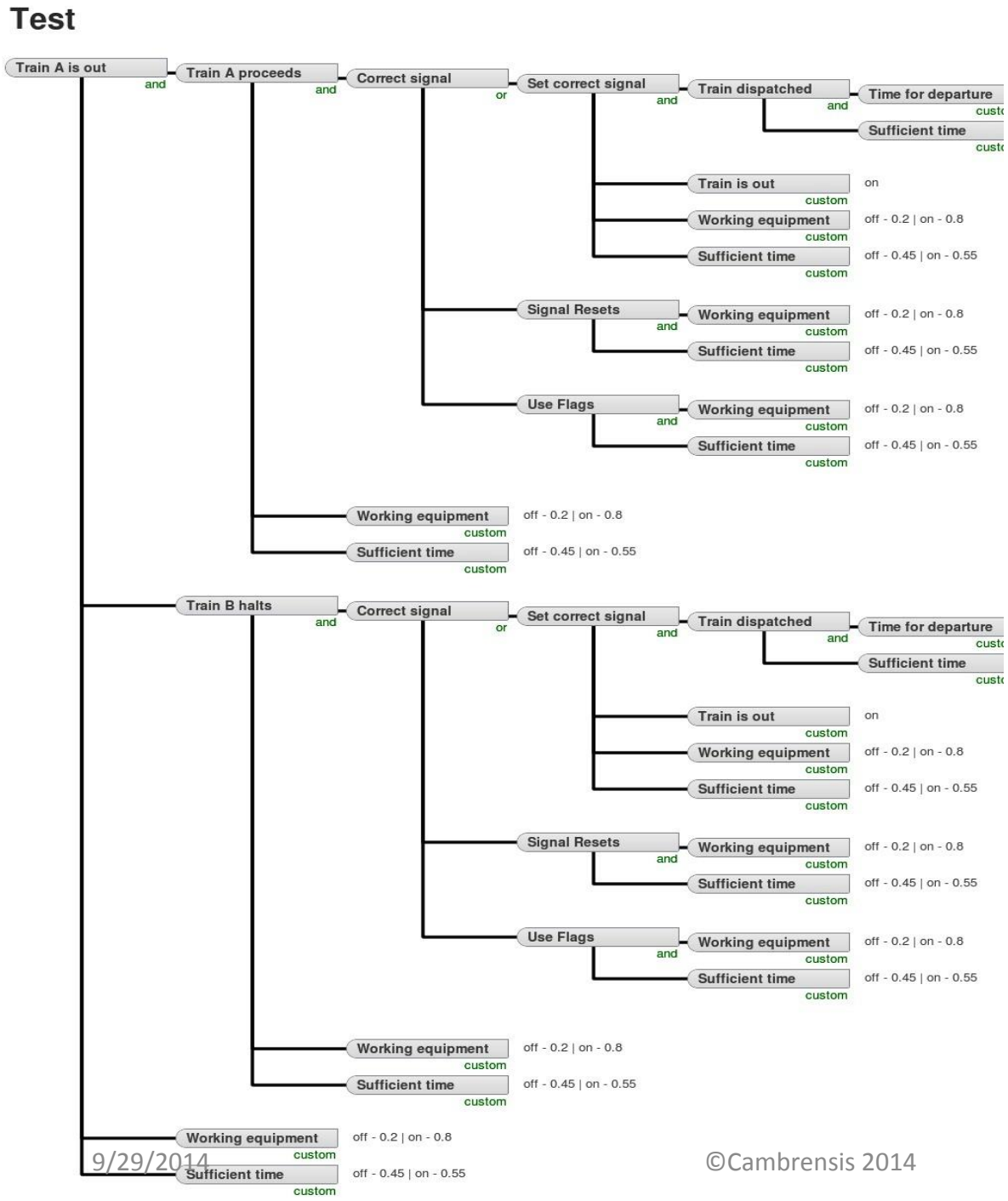
©Cambrensis 2014



Output Probabilities?

- This predicts that on those numbers and this model the probability of a successful outcome is less than 30%
- So we need counter measures!

©Cambrensis 2014



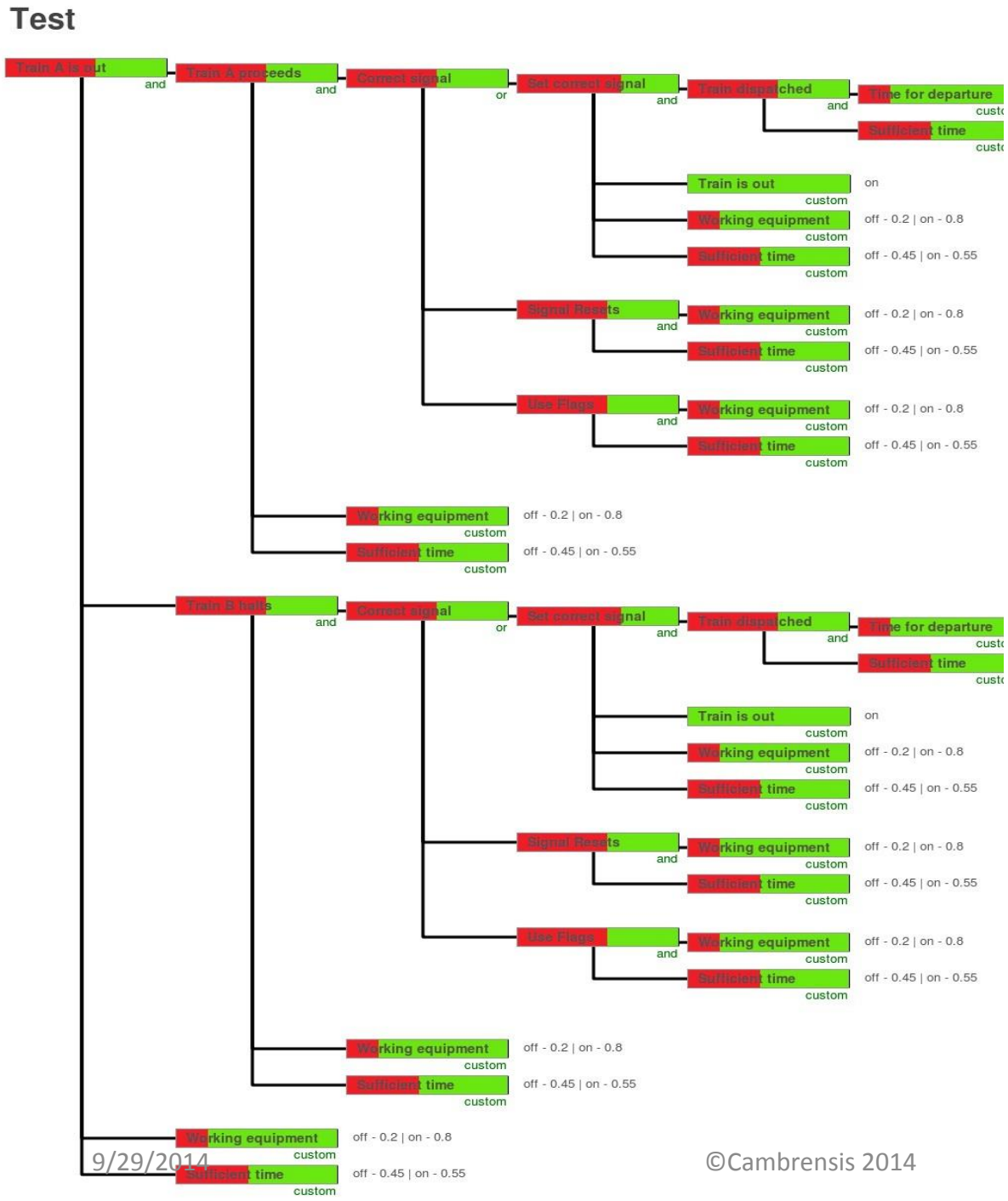
What about the Flags?

The dependency model will now allow us to add the use of flags as an OR dependency

As an alternative to the Correct signal being set, or resetting successfully

This is a normal way to add countermeasures in this kind of study

©Cambrensis 2014



Does it Help?

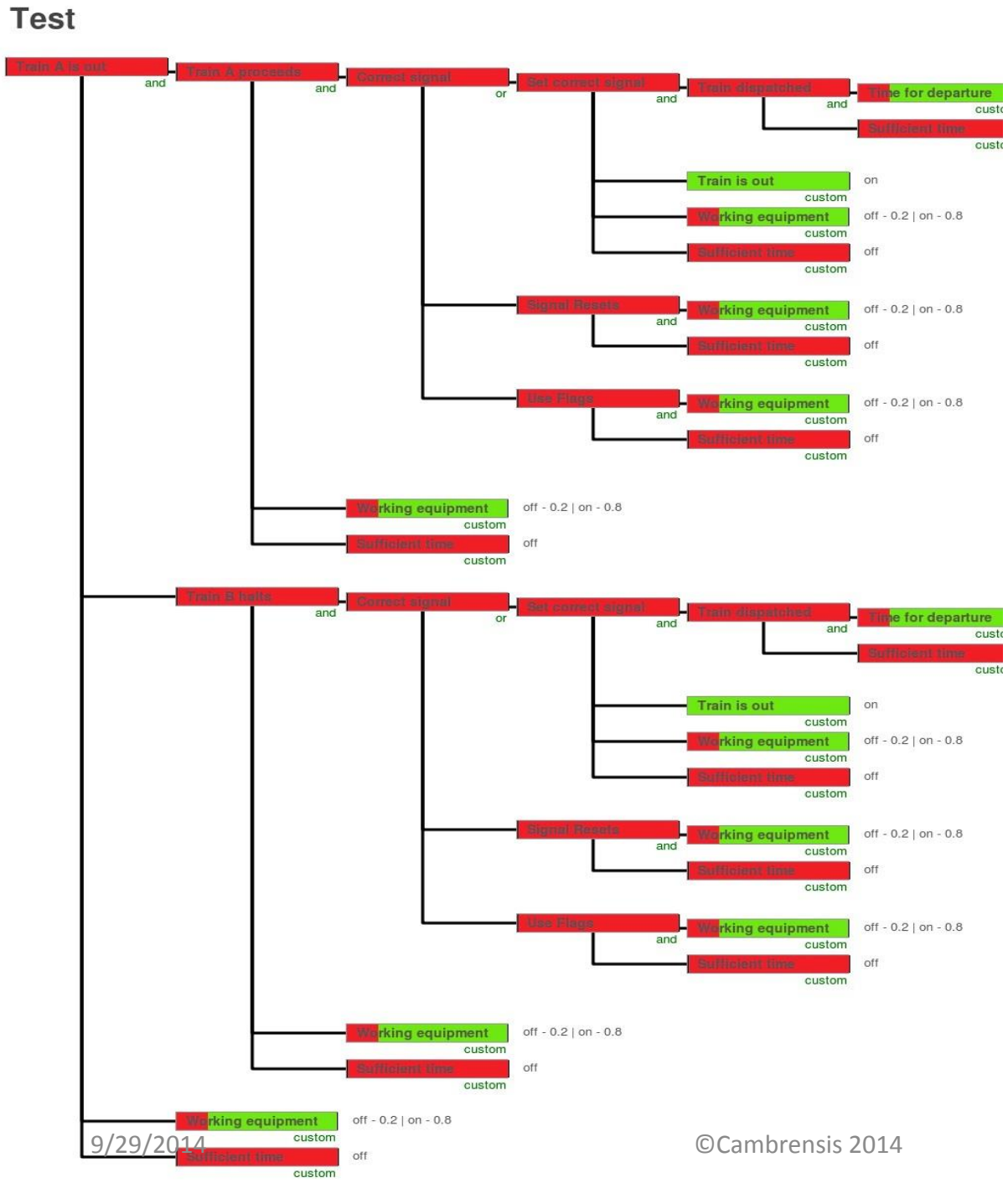
The BBN now predicts the probability of successful Outcomes at some 45%

Significant Improvement but still not effective enough?

How much did it cost

What about alternatives, extras, ranking, prioritisation?

©Cambrensis 2014

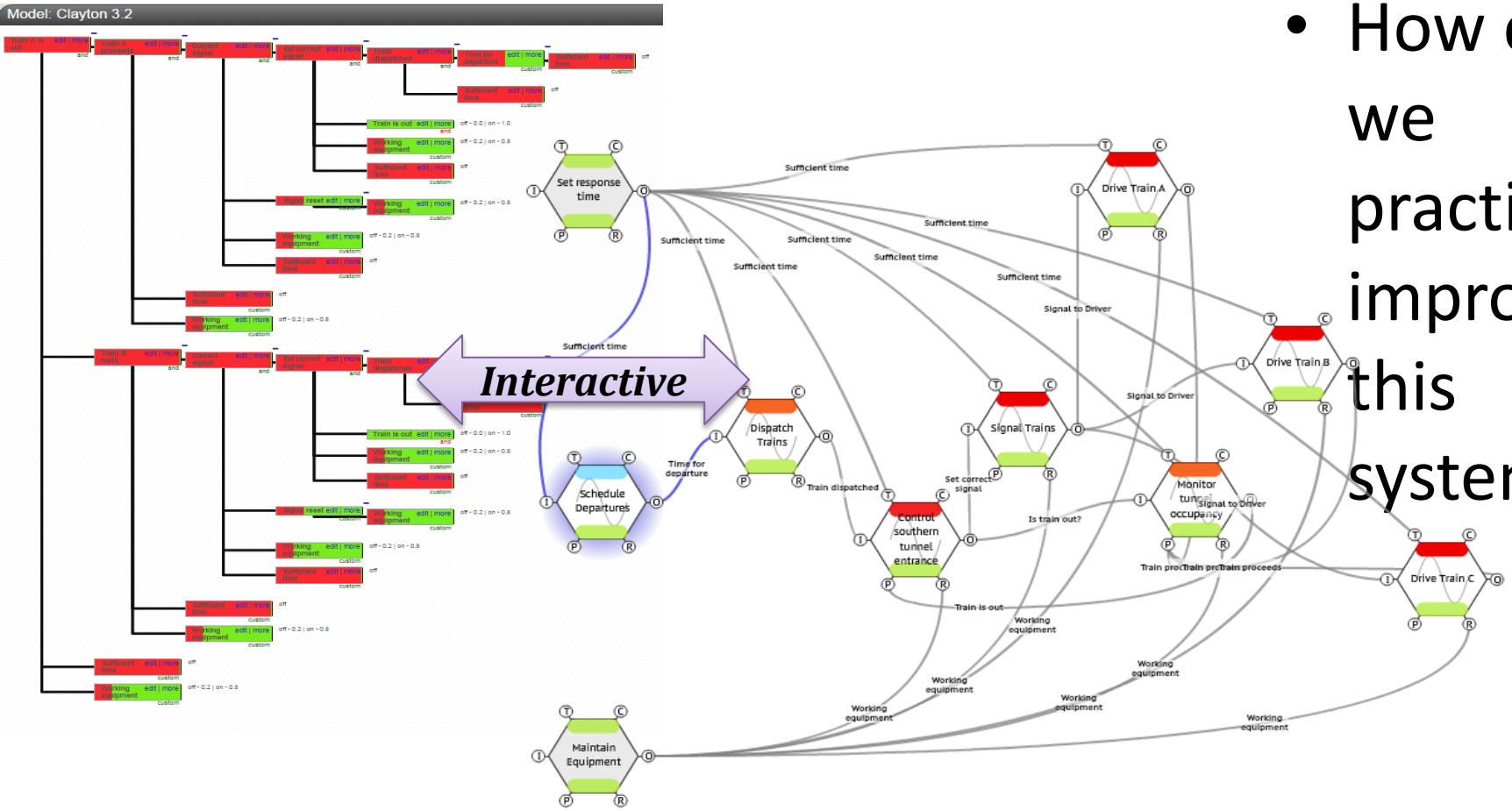


So what is the key issue?

- If we tell the model there is just insufficient Time, it all falls apart!
- It is clear that this is the critical dependency

©Cambrensis 2014

So Back to the Drawing Board and work on the FRAM Visualisation in FMV



- How can we practically improve this system?

©Cambrensis 2014

The lessons from this Analysis?

"Root Cause", (FMEA) "Not enough"– e.g. broken treadle or Signalman reliabilities only part?

- ***Processes/Functions are not independent*** - Complex, sequential Swiss Cheese "Barriers" assume linearity!- e.g. Dispatcher/signal/signalman/ Procedures "Barriers" are not stand alone (BP)
- ***Real Life is much more complicated –*** Complex, Interactive, Emergent – more insight is needed to identify and model systematically, real life , systemic (holistic) behaviours and variabilities. (AS IS?)

©Cambrensis 2014

So What?

- The whole thing is dominated by the system dynamics,(not enough time to react!)
- This also affected the communications (right signal wrong kind of Train!)
- If the driver had not stopped to think – something's wrong? (Near miss?)
- Root Cause – Human Error?
- Signals Passed At Danger (SPAD's)are a recurring, (current) and not resolved problem on UK Railways and normally attributed to "Driver Error"!
- Very Safety I? Don't think, do!

©Cambrensis 2014

So What?

- But the Driver was thinking/ responding.
- Maybe wrong, but human.
- Are Humans a liability and a hazard?(SAFETY I)
- Or a resource for system flexibility and resilience? (SAFETY II)
- You cannot control drivers by expecting (dumb) Pavlovian responses (all the time).
- So a better way is perhaps, to use the driver's ability to react by giving him the right information . (the signalman has an alarm?)
- Tell him the signal's failed (Stop, go and "wait a minute something's wrong"?) (or Fail Safe?)
- He's going to do it anyway (Uberlingen?)

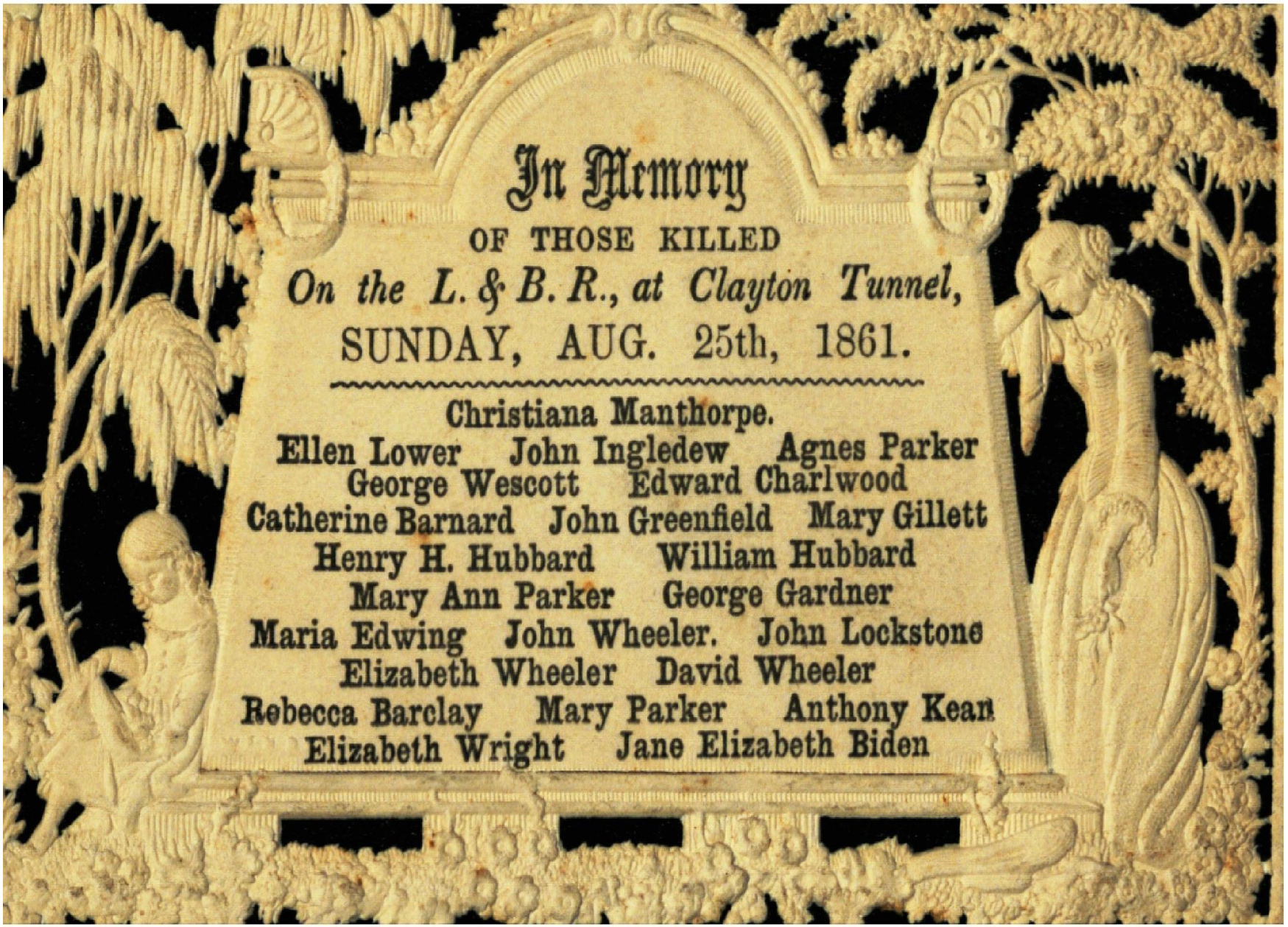
©Cambrensis 2014

Summary

- *We have looked at a simple Victorian Case Study*
- *And concluded it was not so simple!*
- *The fact that People were essential to its effective operation makes it "Complex" by definition!*
- *Thus "simple classical" methodologies might miss the subtleties, such as*
- *"As is" not "as imagined"*
- *The Impact of seemingly independent system interdependencies – the "non linearity"*
- *The Impact of "natural" variabilities – "Resonance"*
- *The crucial importance of "System Dynamics"*
- *Simple approaches can thus give misleading assessments of "System Integrity"*
- *What are the alternatives? Better mousetraps? (to protect the Cheese Slices!)?*
- *This comparative case study suggests –*
- *a SAFETY II, FRAM approach, quantified using integral BBN's*

©Cambrensis 2014

Photo courtesy of http://500px.com/momodem


In Memory
OF THOSE KILLED
On the L. & B. R., at Clayton Tunnel,
SUNDAY, AUG. 25th, 1861.
Christiana Manthorpe.
Ellen Lower John Ingledew Agnes Parker
George Wescott Edward Charlwood
Catherine Barnard John Greenfield Mary Gillett
Henry H. Hubbard William Hubbard
Mary Ann Parker George Gardner
Maria Edwing John Wheeler. John Lockstone
Elizabeth Wheeler David Wheeler
Rebecca Barclay Mary Parker Anthony Kean
Elizabeth Wright Jane Elizabeth Biden