Closer Running: Magic Potion or Deadly Poison?

Hongsin Kim, Teaching Fellow, University of Birmingham
Felix Schmid, Professor of Railway Systems Integration, University of Birmingham
Phillip Dakin, Railway Systems Engineer, Bechtel
Shuxia Lu, Engineer, Siemens Mobility

SUMMARY

Limited and variable adhesion at the wheel-rail interface is a fundamental characteristic of railway systems, leading inevitably to extended stopping distances. Traditionally fixed block methods of railway control have been and are being used to overcome this impediment to safe operation. However, this solution prevents railways from making full use of the infrastructure. Increases in demand for rail travel and the difficulty of adding infrastructure, has prompted the development of a philosophy that involves trains being separated by less than a full braking distance, a concept that is like motorway driving. This is based on the premise that it is highly unlikely that a train stops instantly, over a near zero distance. Therefore, using the full braking distance in a system design could be deemed an overly cautious approach.

In this paper, the authors critically review the research into closer running of trains and conduct a safety analysis of the approach. For the safety analysis of the system, the authors compare two approaches: (1) an event chain accident causation model based on a classical Event Tree Analysis (ETA) and (2) a systematic theory accident causation model, which is a relatively novel approach.

1 INTRODUCTION

Britain's rail industry has a plan to double the capacity of the rail network but intends to achieve this objective without building new lines, which are both costly and environmentally damaging. The capability required to achieve this significant increase in capacity is expected to come from the 'closer running' of trains. The closer running of trains is not a new endeavour. For many years, the railway has strived to increase capacity through reductions in the technical headway, the distance or time between a first train and the following trains. The strategic positioning of signal boxes during the absolute block era and the adoption of 4 aspect colour light signalling as part of the refinement of multiple-aspect signalling on mainline railways and the introduction of moving block on metros are examples.

It is recognised increasing capacity on the railway system further requires a move away from infrastructure-based railway control systems, such as those relying on lineside signalling, to train based moving block systems with minimal trackside equipment (Winter, 2009). It must be noted that lineside signalling does not directly limit capacity. However, it is intrinsically linked to the fixed block approach to railway control, which constrains capacity by requiring a full braking distance between all trains and by using relatively coarse infrastructure-based train detection. Such systems are optimised for a particular line-speed and result in inefficient use of the infrastructure. When using a moving block system, trains can operate at a separation distance that is appropriate for the speeds at which they are travelling, eliminating the loss of capacity created by the limitations of fixed block working. The method proposed for achieving moving block operation on mainline railways in Europe is the European Train Control System Level 3 (ETCS L3), which has characteristics similar to those of metro type Communications Based Train Control or CBTC.

Bodies such as the IRSE International Technical Committee (2016) acknowledge that technologies are now emerging that will allow the railway to adopt new methods of operation, described as 'closer running' or 'ETCS Level 4'. This concept educes the gap between trains, when compared to ETCS L3, by adopting the concept of relative braking distance, advocated by Emery (2011), for example. With this method of operation, trains can be brought closer together on the assumption that trains decelerate at a predictable rate and, thus, if a following

train is aware of the preceding train's speed and precise deceleration rate, it can be operated at a separation distance that is less than the full braking distance. In theory, this can lead to headway times at levels that are close to the response times of the braking systems, with allowances for the accuracy of train location and the communication system latency. The RSSB (RSSB, 2017) has coined the term 'motorway driving' for this method of operation. It is believed that this approach will add significant capacity, however, it will also bring changes to the philosophy of railway operations.

The authors argue that implementing such a concept would provide only a limited increase in capacity at junctions and in stations while the benefit would be greater on plain line. At junctions, a service on a diverging route would not be improved by 'closer running'. This is because the following train must maintain a full braking distance to the point of divergence until the switch-blades are set and locked in the new position. At stations, the dwell time is the main component of the headway. Since the front train is dwelling at zero velocity, both a relative moving block and an optimised absolute moving block will have the same headway (Williams, 2016). Due to these limitations, the concept may not bring benefits for railways with closely spaced junctions and stations. A team at the Birmingham Centre for Railway Research and Education (BCRRE) is conducting research on the introduction of S&C technologies that might enhance the benefits of 'closer running' in junction areas but this is outside the scope of the present paper. Instead, we focus on plain line operations, where most of the benefits of 'closer running' are expected to accrue (Emery, 2011).

There are concerns that a catastrophic event might occur when a preceding train stops near-instantaneously, e.g., because of colliding with a landslide or a similar immovable object. According to the IEC functional safety standard IEC 61508 (IEC, 2010), a safety analysis must be performed early on in the system life cycle to reduce systematic risks and to reduce cost. For the present paper, the authors applied two types of analysis to investigate the risk involved in 'closer running'. For approach (1), an Event Tree Analysis (ETA) and Boolean algebra were applied to quantify the probability and consequences of an accident. They used historic data from industry statistics and reports covering a 10-year period. This investigation revealed the following events as having the potential to decelerate a train very rapidly, i.e., at rates much greater than emergency braking: fallen trees, collisions with heavy road vehicles and fully-grown cattle, engineering work sites, track plant and, most importantly, avalanches, landslides and large scale debris.

For approach (2), the authors extended the Unified Modelling Language into a sequence diagram meta-model for a Systems Theoretic Process Analysis (STPA), to assess the safety of the 'closer running' approach. The authors pinpointed hazards in operational scenarios, built the associated model and identified the unsafe control actions (UCA) that could lead to the hazards. For each unsafe control action, the authors then established the causal scenarios that would lead to the unsafe control actions and proposed mitigations or solutions. However, They applied the systematic theory accident causation model to just one hazard analysis. Further research is therefore required to adapt the method for more in-depth safety analyses.

2 REVIEW OF SAFETY ANALYSIS METHODOLOGIES

An accident causation model is intended to explain how accidents happen. There are two types of safety analysis methods that can be applied to railway control systems, namely, chain-of-events based methods and system theory-based methods. Event based safety analysis methods, such as Fault Tree Analysis (FTA), Failure Modes and Effects Analysis (FMEA), Failure Mode and Effects Criticality Analysis (FMECA) and ETA, consider an accident as the result of a chain of events (Benner, 1975). The choice of events and the analysis end points are usually subjective and relationships between causal factors are assumed to be linear. Social and organizational factors and software error are not considered in this type of accident causation model. However, it works well for physical component failures as triggers. By contrast, Systems Theoretic Accident Model and Process (STAMP) is based on system theory and considers interactions between system components. STAMP includes three main methodologies, i.e., STPA, AcciMap and FARM. STPA is an accident causation model proposed by Leveson in 2004, which has been adopted relatively widely. In this method, accidents are considered to result from inadequate enforcement of constraints on the interactions between subsystems and other entities (Leveson,

2004). It offers a more comprehensive understanding of system safety and works well for finding software and design errors.

2.1 Event-based Accident Models

The methods used most commonly by industry are Hazard and Operability Studies (HAZOP) (IEC, 2016), FMEA (IEC, 2006) and FTA (IEC, 2006). These methods can be applied to different phases of the system lifecycle, either individually or in combination. In addition, safety is evaluated through the concept of 'risk', or its absence and, if the acceptable risk, the system is assessed as safe.

These methods are easy to understand and carry out. Therefore, they are widely accepted and applied in the railway industry. FMEA has been adopted to analyse the subsystems of ETCS Level 1 and ETCS Level 2 to derive the respective safety requirements (ERA, 2016). Additionally, because FTA can be used to describe and calculate risks, it is also being used to apportion the Tolerable Hazard Rate (THR) for functional failures of ETCS (UNISIG, 2016). A series of HAZOP studies were conducted and these identified hazards and operability issues related to Enhanced ETCS Applications (RSSB, 2006).

However, purely technical assessments are not sufficient since many systems today are socio-technical in nature and integrate complex interactions among people, technology and management. Given the occurrence of catastrophic accidents in recent years, the chain-of-events based methods are arguably inadequate to carry out safety analyses for socio-technical systems (Lindberg, et al., 2010). Some scholars believe that these methods oversimplify the progression towards accidents and that they omit non-linear interactions among non-failed components (Leveson, 2011b). Therefore, safety analysis methods have been proposed that are based on system theory and these have gradually become predominant in academia.

2.2 Systematic Theory Accident Causation Model

STAMP has been successfully applied in many safety-critical areas, including aerospace, the defence industry, transportation and the chemical industry. The systematic theory accident causation model treats safety as an emergent system property, that is, as the result of interactions among the system components and, thus, views the system as a whole. Compared with chain-of-events causation model, systematic theory-based methods believe that accidents are caused by inadequately managed or controlled interactions between components rather than individual failure events. STPA is a safety analysis method or accident causation model, based on STAMP, that was proposed by Leveson in 2002 (Leveson, 2002) and further developed by her in later publications (Leveson, 2011a) (2011b). In the systematic theory, emergent properties of a system are controlled by constraining the interactions between components and controlling the behaviour of each component. Therefore, STAMP transforms safety issues into control issues and the goal is to ensure that all constraints are met, thereby ensuring system safety. If the safety constraints are not meet during system development, design and operations, accidents will occur. As a result, when analysing system accidents with STAMP, the objective is to find issues associated with safety constraints throughout all stages of the system life-cycle.

3 EVENT TREE ANALYSIS OF THE CONCEPT OF CLOSER RUNNING

To maintain the required levels of safety and to comply with legislation, the risk associated with new or modified systems must be made as low as reasonably practical (ALARP), see Health and Safety Executive (HSE) (2001). To determine what is reasonably practical, the level of risk must first be evaluated. This can be achieved using a quantified risk assessment, as described by Smith (2011). Smith states "The term Quantified Risk Assessment (QRA) refers to the process of assessing the frequency of an event and its measurable consequences (e.g., fatalities and / or damage)" (Smith, 2011). The authors have used an event tree analysis to determine the probability or frequency of a collision event caused by 'closer running' and accident reports from previous incidents to determine the likely consequences. This is known as the 'concrete block scenario, as defined by RSSB (2017). The authors' quantified risk assessment is based on data from 2006-2016.

To quantify the risk the authors have used the methodology illustrated in Figure 1:

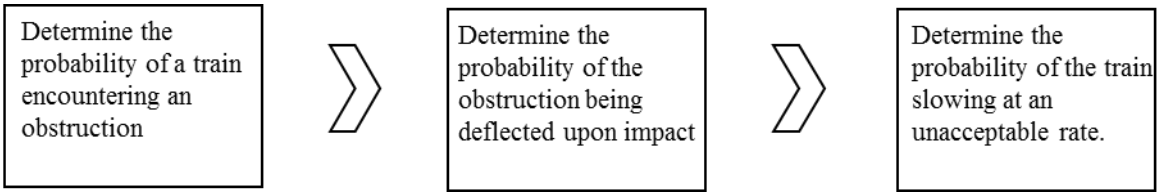

Figure 1: Risk assessment methodology adopted for this study (Authors, 2018)

Figure 2 is an event tree model that shows all outcomes that can result from a situation where a train strikes an object on the track, e.g., a truck or debris from a landslide.

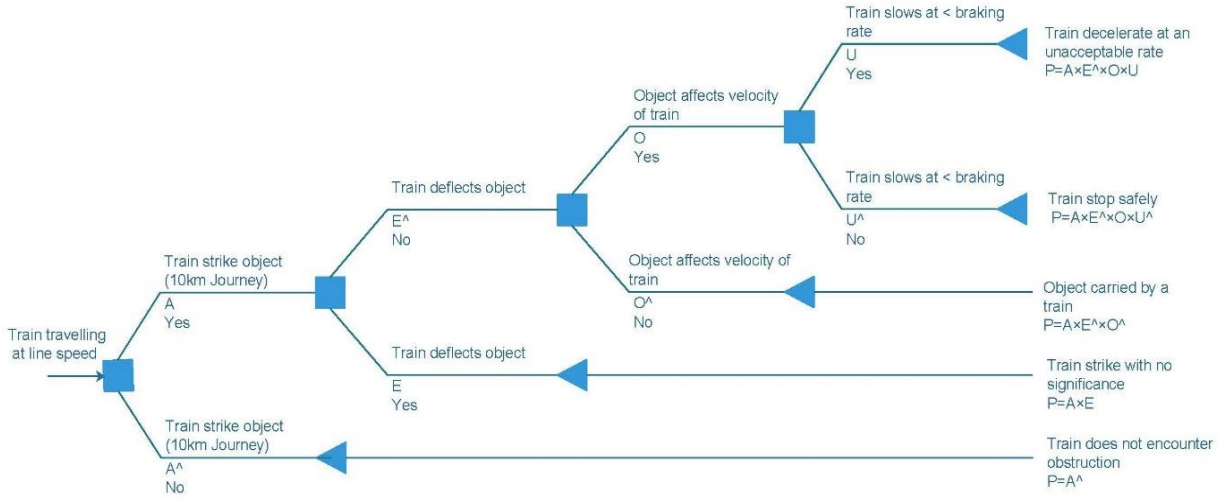

Figure 2: Event Tree Analysis of obstacle collision scenario (Authors, 2018)

3.1 Probability of Encountering and Deflecting an Obstruction

To determine the probability of a train encountering an obstruction, the authors gathered industry data for a range of obstruction types and calculated the associated risk. Using data from RSSB (2017), the authors established that the average passenger train kilometres (ptkm) per annum had amounted to 514 million during the period 2011-2016. Table 1 shows a summary of the collision incidents, produced by the authors, based on the published data.

Table 1: Accidents involving obstructions (RSSB, 2017) summarised by the authors

Nature of Incident / Accident	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016
Collison with road vehicles not at level crossings*	2	4	1	0	3
Struck by large falling object*	0	0	0	0	0
Striking animals*	190	346	294	325	301
Striking other objects*	199	184	214	184	169
Totals	391	534	509	509	473
*Aggregate figure for passenger and non-passenger trains					

Using annual passenger train kilometre data for 2019 (ORR, 2019) and the incidents listed in Table 1 (total number of accidents involving obstructions) results in the typical train kilometres per incident shown in Table 2.

Table 2: Millions of passenger train kilometres per incident (Authors, 2019)

Year	Passenger train kilometre (million)	Total number of incidents involving obstructions	Passenger train kilometres per accident (ptkm)
2011/12	509.9	391	1,304,092
2012/13	510.2	534	955,431
2013/14	510.6	509	1,003,143
2014/15	517.5	509	1,016,699
2015/16	521.8	473	1,103,171
		Mean	1,076,507

The probability of a train encountering an obstruction on the line during a theoretical 1 km journey becomes:

$$\frac{1\ \text{km}}{\text{Mean value of Passenger train kilometres per accident}} = \frac{1}{1{,}076{,}507} = 9.29\text{E}{-}07$$

For the commuter who makes a short journey, e.g., a 10 km average daily journey, the probability of an incident during a journey is $9.29\text{E}{-}06$. For the passenger who travels further, e.g., a 330 km average daily journey, the probability increases to 3.07E-04 and for the long distance traveller, e.g., making a 2000 km, the probability to encounter an obstruction increases to 1.86E-03 per journey.

Conversely, the probability of each type of journey not being affected by an obstruction can be expressed as:

- 1 km 100-0.00000093 99.99999907
- 10 km 100-0.00000928 99.9999907
- 330 km 100-0.00030653 99.9969346
- 2000 km 100-0.00185779 99.9981422

This data forms the basis for the **first decision node** in the event tree of Figure 2.

3.2 Probability of Deflection and Consequences

For the object to represent a hazard in the context of this study, it must be capable of resisting deflection and, thus, be able to stop or derail a train. The authors have used records of previous incidents from the annual and monthly railway accident reports, published by the Rail Accident Investigation Branch (RAIB), to determine the likelihood of an object being deflected upon impact. This is complex due to the diversity of objects that cause obstructions and the diversity of rolling stock operating on the GB infrastructure. The consequences of each scenario thus depend on the characteristics of the object and of the train and on other variables involved in the event, e.g., train velocity, mass. The authors recognise, therefore, that the probabilities provided have a degree of uncertainty.

The rail accident reports produced between 2006 and 2016 suggest that the causes of incidents can reasonably be divided into eleven categories. The issues associated with two of these categories of incidents are discussed in the following sections. In both cases, N^i is the number of occurrences and Nt^{km} is the number of train kilometres.

3.2.1 Dislodging of Payload

There is clear evidence that occurrences of payload movement have not diminished during the past 10 years and the authors suggest that the risk has actually increased due to the growing rate of container detachments. GB

data suggests that 5 traffic disruptions occurred due to payload falling from trains between 2006 and 2016, with examples shown in Table 10 in the appendix.

The probability of a train encountering an obstruction caused by fallen payloads during a 1 km journey can be expressed as:

$$\frac{N^i}{N^{tkm}} = \frac{5}{2570 \times 10^6} = 1.9 \times 10^{-9}$$

The 5 incidents identified led to damage to engineering vehicles and infrastructure but there appear to have been no occurrences of a train colliding with a dislodged container on the GB mainline network. However, payload movement has caused serious accidents in other countries, such as the 2 January 2019 accident on the Great Belt Link in Denmark, where a passenger train collided with a semi-trailer that had become detached from its pocket wagon, causing nine deaths. Therefore, we cannot conclude that there is no hazard. Furthermore, the probability of a train deflecting an obstruction caused by a dislodged payload cannot be calculated, due to a lack of data.

3.2.2 Infrastructure Component Failure

The sample of data in Table 11 in the appendix shows that no asset is immune from failure and, even those presenting no obvious hazard, such as platforms, are potential obstructions. The probability of a train encountering an obstruction caused by failed infrastructure during a 1 km journey can be calculated in the same manner as 2.8×10^{-9}.

The authors postulate that the failed infrastructure items listed in Table 11 do not possess the mass to slow a train at an unacceptable rate, so all would be deflected upon impact. The probability of deflecting a failed infrastructure component failure is therefore expressed as:

$$2.8 \times 10^{-9} \times 1 = 2.8 \times 10^{-9} \text{ per 1 km journey.}$$

However, outside the period discussed here, a train collided with a collapsed footbridge, at Barrow-on-Soar, on 1 February 2008. The train stopped in a very short distance and passengers were injured. Infrastructure failures tend to lead to derailments and gauge infringement. A typical example is a freight train derailment near Moscow, caused by a track failure that was due to inadequate maintenance. A passenger train hit the obstacle and 9 people were killed and many injured (BBC, 2014).

3.2.3 Summary of the Risks associated with the 11 Categories of Incidents

The data shown in Table 3 forms the basis of the 2nd decision node in the event tree shown in Figure 2.

Table 3: Summary of Likelihood of Deflection (Authors, 2018)

Category of Obstruction	Number of collisions	Number deflected	% chance of obstacle being deflected
Payload dislodged from train	0	0	N/A
Failed infrastructure component	4	4	100
Snow	1	0	0
Landslide	9	0	0
Fallen tree	1	0	0
Road vehicles	2	1	50
Animals	1456	1455	99.93
Vandalism	108	108	100
Equipment from engineering work	3	1	33.33

Debris or rubbish	3	0	0
Engineering plant	3	1	33.33

It is important to note that the lessons that can be drawn from the values shown in Table 3 are limited and are not representative for other countries and situations.

3.3 Probability of Affecting Train Stopping Distance

A train decelerating at greater than its predicted braking rate creates a significant hazard when operating under 'closer running', because it is likely that a following train will not have sufficient braking capability and, therefore, a collision is likely to occur. The authors have assessed which of the obstructions could slow a train at a rate greater than those commonly used on the GB mainline railway, where Railway Group Standard GM/RT2045 (superseded GM/RT2044) provides the stopping distances that can be expected (RSSB, 2016).

The minimum braking distances stated in GM/RT2045 have been specified to prevent damage to wheels and track when the maximum braking rate is applied and the authors suggest that this requirement must be maintained. Again using the data available from industry incident reports, the authors have analysed which obstructions affected the speed of trains upon collision. They have also analysed the stopping distances involved in these collisions to establish which had the potential to slow trains at greater than permitted braking rate.

Table 4 Likelihood of different Types of Obstruction affecting Train Speed (Authors 2019)

Type of Obstruction	Number of collisions during review period	Number which affected train speed	% chance of affecting speed
Payload shifted / fallen from train	0	0	N/A
Broken infrastructure component	4	0	0
Snow	1	1	100
Landslide	9	9	100
Fallen tree	1	1	100
Road vehicles	2	2	100
Animals	1456	1	0.07
Vandalism	108	0	0
Materials from engineering work	3	2	66.66
Debris or rubbish	3	3	100
Engineering plant	3	2	66.66

The historical data suggests that the 'concrete block scenario' will not occur as a result of payloads shifting and falling from trains. However, the authors recommend that it should be assumed that trains cannot deflect full containers, to ensure that the risk model is as robust as possible, so that decisions around this scenario do not erode safety. Of the 7 obstructions analysed in 3.2.2, none had the potential to slow a train at an excessive rate without causing derailment. However, the authors also reviewed data associated with a collision with snow in Summit Tunnel (RAIB, 2011). The minimum recommended braking distance for multiple units travelling at 75 mph (33 m/s) is currently 399 m, according to Railway Group Standard GM/RT2045 (RSSB, 2016), formerly GM/RT2044 (RSSB, 2001). A comparison of the stopping distance in (RAIB, 2011) and the recommended minimum stopping distance stipulated yields a difference of 145 m (399 m-254 m), showing that the train involved in this collision slowed at an unacceptable rate.

Based on the data analysis shown in Table 5, the probability of a train slowing at an unacceptable rate when obstructed by a landslide can be expressed as:

$$\frac{N^{ud}}{N^{il}} = \frac{4}{7} = 0.57$$

Where N^{ud} is the number of unacceptable decelerations and N^{il} is number of instances of hitting landslides.

Table 5: Summary of Landslip Collisions and Analysis of Deceleration Events (Authors, 2018)

Incidents (Year of accident)	Merstham Tunnel (2017)	Kemble (2007)	Gillingham Tunnel (2010)	St Bee's (2012)	Rosyth (2012)	Falls of Cruachan (2012)	Bargoed (2013)
Line speed (mph)	82	90	85	60	65	30	30
Train speed on impact (mph)	70	51	64	47	45	30	30
Stopping distance (m)	320	243	404	121	160	N.A.	15
Recommended braking distance (m)	351	189	306	156	156		76
Evidence of train decelerating at an unacceptable rate	Yes	No	No	Yes	No	Yes	Yes

The data from Table 4 forms the basis of the 3rd decision node and the data from Table 6 forms the basis of the 4th decision node shown in the event tree in Figure 2.

Table 6: Likelihood of unacceptable Deceleration Events (Authors, 2018)

Type of Obstruction	Number of collisions occurred	Number of unacceptable decelerations	% chance of unacceptable deceleration
Payload shifted / fallen from train	0	0	-
Broken infrastructure component	3	0	0
Snow	1	1	100
Landslide	7	4	57
Fallen tree	1	0	0
Road vehicles	2	0	0
Animals	1456	0	0
Vandalism	108	0	0
Materials from engineering work	3	0	0
Debris or rubbish	3	2	66.66
Engineering plant	3	1	50

3.4 Data Analysis and Discussion

3.4.1 Event Tree Analysis

The investigation into historical incidents has revealed that collisions with obstructions caused by snow, landslides, road vehicles and debris have the potential to slow trains at unacceptable rates. The associated probabilities have been calculated using the process illustrated in Figure 3 and are listed in Table 7.

Table 7: Event probability during a 1 km journey (Authors, 2019)

Event	**Probability**
Train does not encounter an obstruction	0.99999907
Train strikes obstruction with no significant effect	3.87429E-07

Object / obstruction deflected by train	1.98907E-07
Train stops safely at an acceptable rate	2.49604E-07
Train decelerates at an unacceptable rate	9.40610E-08

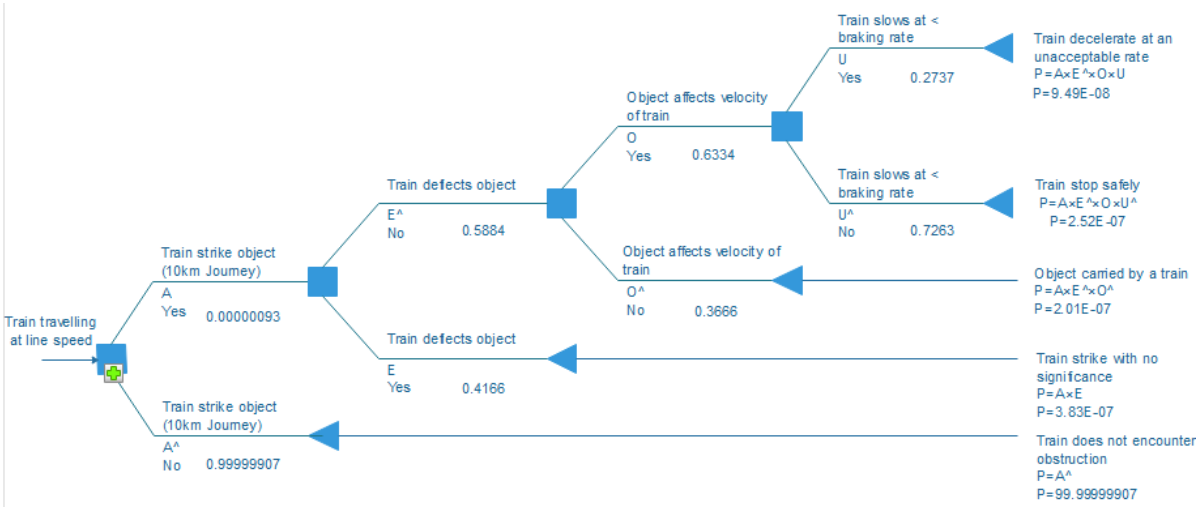

Figure 3: Event tree analysis for probability of trains slowing at unacceptable rates due to obstructions (Authors, 2018)

3.4.2 Risk Analysis and Discussion

Before proceeding into a discussion about 'how' the risk can be reduced through mitigations, the authors suggest that one must first consider 'why' the risk is to be reduced. Using data from **Error! Reference source not found.** a nd assuming a 1 km journey, a train will decelerate at an unacceptable rate as a result of hitting an obstruction once in 10.63 million journeys:

$$\frac{1}{9.4061\text{E}{-}08} = 10{,}631{,}397 \text{ or once in 10.5 million km}$$

Eurostat (2017) states that an average rail passenger in the UK travels approximately 990 km each year. Therefore, the number of years it would take for this average passenger to be exposed to their train decelerating at an unacceptable rate due to an obstruction is:

$$P^1 \times n^{pkm} = 9.49 \times 10^{-8} \times 990 = 9.39 \times 10^{-5} \text{ or once in 10,648 years}$$

The result indicates that the risk associated with the concrete block scenario on the UK mainline railway falls into the region of negligible / tolerable. Based on historic incident data, the probability of a train not deflecting an obstruction (Section 3.2.1) caused by a dislodged payload is 0 in the UK. However, we cannot conclude from this observation that the risk does not exist. For example, in the Great Belt Bridge rail accident of 2 January 2019 in Denmark a train following another at less than braking distance would have collided unavoidably with the multiple unit involved in the accident.

The Barrow Upon Soar collision between a train and a collapsed footbridge in 2008 near Loughborough illustrates the situation. It resulted in the train stopping in less than 1/3 of the normal braking distance (RAIB, 2008). The footbridge had been accidentally demolished by a lorry. It is likely that a 'closer running' following train would have collided with the train involved in the collision.

The event tree analysis in Figure 3 visualises the sequence of events that leads to a situation where a train slows down at an unacceptable rate. One of the drawbacks of this method is that only certain initiating event can be

studied in the analysis and that it tends to overlook subtle system dependencies and is thus not ideal to handle common cause failures in quantitative analyses.

4 STPA MODELLING METHOD BASED ON UML EXTENSION AND CASE STUDY

The approach discussed in section 3 is limited to analysing basic interaction relationships and, because it is not systematic, it has poor traceability and coverage. Therefore, the authors believe that systematic theory-based methods are more suitable for a complicated and complex system like the railway. Thus, for approach (2), the authors extended the Unified Modelling Language into a sequence diagram meta-model based on STPA, to analyse the safety of 'Closer Running'. The authors identified hazards in some operational scenarios, built the associated models and established unsafe control actions (UCA) that could lead to hazards. For each unsafe control action, the authors further identified the causal scenarios that lead to it and propose mitigations or solutions. The systematic theory accident causation model based methods are applied to only one hazard analysis.

4.1 STPA Methodology

4.1.1 STPA Procedures

As shown in Figure 4, the following are the specific steps to follow in STPA procedures:

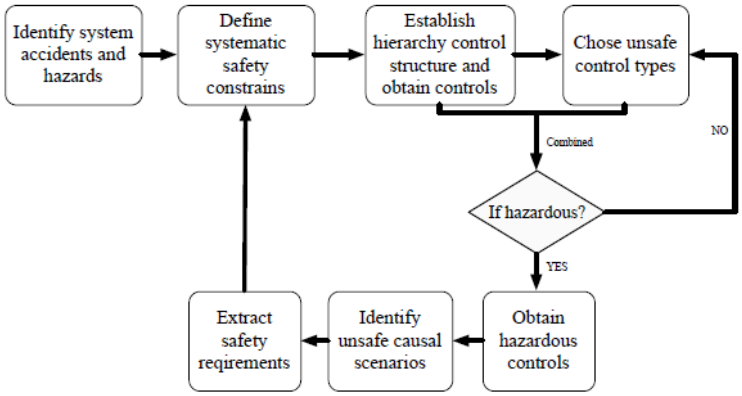

Figure 4: STPA Procedures

- Step 1: Identify system operational scenarios and potential accidents;
- Step 2: Combined with system accidents and operational scenarios, identify system hazards for each operational scenario;
- Step 3: Establish the system control structure by means of an extended UML sequence diagram, which is the basis for unsafe controls identification. Modelling details can be found in Section 4.1.2;
- Step 4: Identify unsafe control actions (UCA), based on the four general types of UCA provided by the STPA standard, that could push the system into a hazardous state;
- Step 5: Identify unsafe casual scenarios that lead to unsafe control actions. Causal scenarios describe how human, equipment and environment interact with each other and result in unsafe control actions;
- Step 6: Propose safety requirements to mitigate or solve the causes. Designers could modify the system structures based on these safety requirements and the analysis is then iterated from Step 3.

4.1.2 Extended UML Sequence Diagram

A UML sequence diagram describes how instantiations interact with each other and emphasises the time-order of messages, which makes up original STPA model static nature to some extent. Therefore, a UML sequence diagram was chosen to create the standardised and unified STPA control structure shown in Figure 5.

The authors added STPA control structure elements to the UML sequence diagram meta-model to form a new UML meta-model. In the STPA model, the smallest control loop includes a controller, actuator, sensor and a controlled item. The overall control structure consists of many small control loops. Therefore, the instantiation specification in the UML meta-model can be extended to a 'controller instance', 'actuator instance', 'controlled object instance' and 'sensor instance'. In addition, the interactions between instantiations is achieved by sending messages in a UML sequence diagram. Therefore, by combining STPA modelling elements, the message can be extended to 'command', 'communication', 'feedback' and 'disturbance'. The fully extended version of the UML sequence diagram is shown in Figure 6.

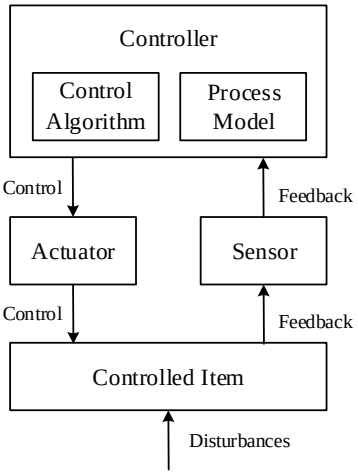

Figure 5: A Standard Control Loop (Authors, 2018)

The control loop based on the extended UML sequence diagram in Figure 6 is presented in Figure 7.

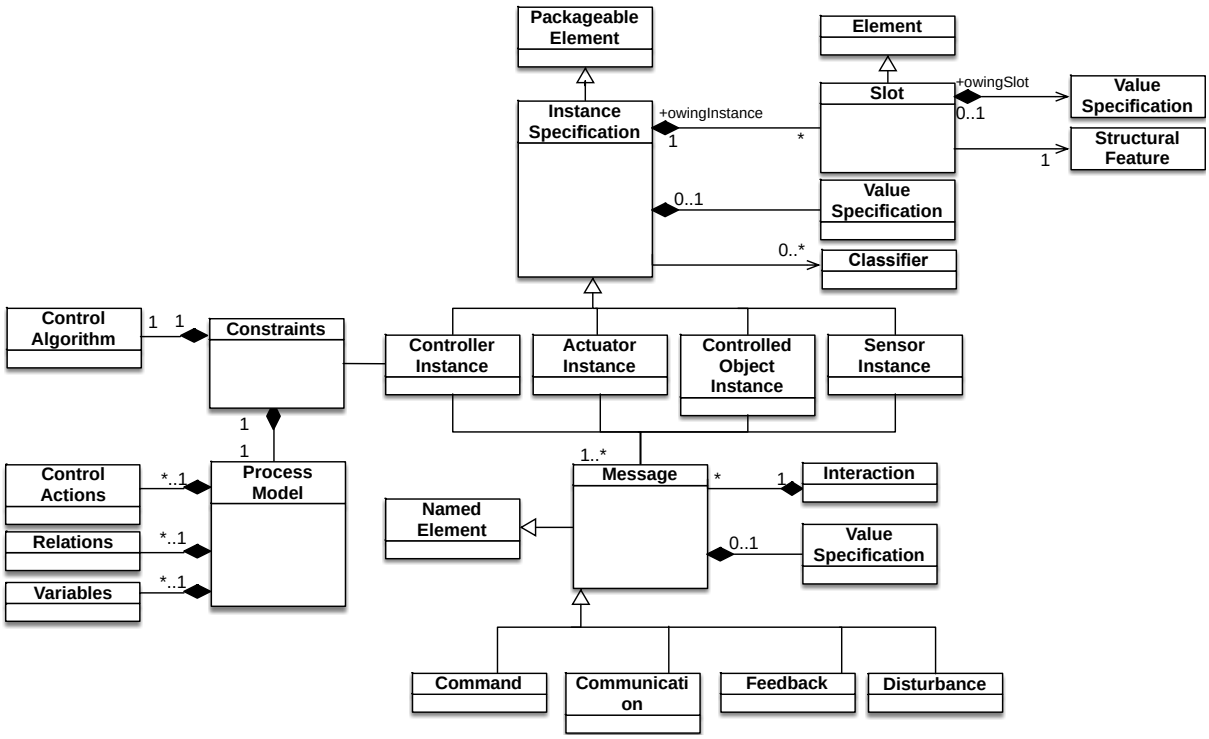

Figure 6: Extension of the UML Sequence Diagram (Authors, 2018)

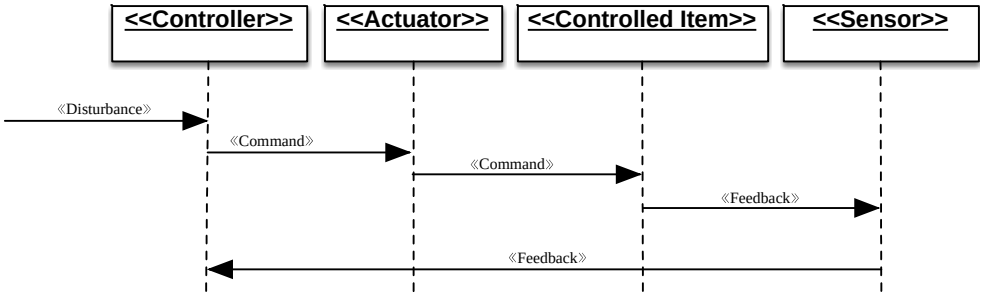

Figure 7: Extended UML sequence diagram of the STPA model (Authors, 2018)

4.2 Case Study for 'Closer Running' or ETCS Level 4

For this section, the authors selected the operational scenario 'a train convoy runs on plain line' to perform the STPA safety analysis based on the extended UML sequence diagram.

4.2.1 Accidents and Hazards Identification

Generally, railway incidents can be classified depending on their consequences (head-on collisions and rear-end collisions) and causes, such as train derailments due to over speed or train collisions with obstructions.

For the scenario 'a train convoy runs on plain line', seven hazards are identified as follows:

- Hazard 1: A following train collides with the leading train on plain line;
- Hazard 2: A train convoy collides with a train on plain line;
- Hazard 3: A train convoy exceeds the safe speed and derails on plain line;
- Hazard 4: A following train exceeds the safe speed and derails on plain line;
- Hazard 5: A leading train exceeds the safe speed and derails on plain line;
- Hazard 6: A leading train collides with an obstruction on plain line;
- Hazard 7: A following train collides with an obstruction on plain line.

4.2.2 Model Building based on the Extended UML Sequence Diagram

The hierarchical control structure for 'closer running' or 'ETCS Level 4' is shown in Figure 8. The control system is based on train-to-train communication and has three levels, a wayside control subsystem, an onboard control substructure and a train level subsystem. The arrows in the figure show the information flows between the components. A Radio Block Centre (RBC) receives information from the trains, the adjacent RBCs and stations to generate a Movement Authority (MA). The MA is sent to the trains by a wireless communication system. The front train shares its position, speed information and the rate of change of speed with the train in rear and its acceleration and deceleration are thereby controlled by the front train in 'closer running'.

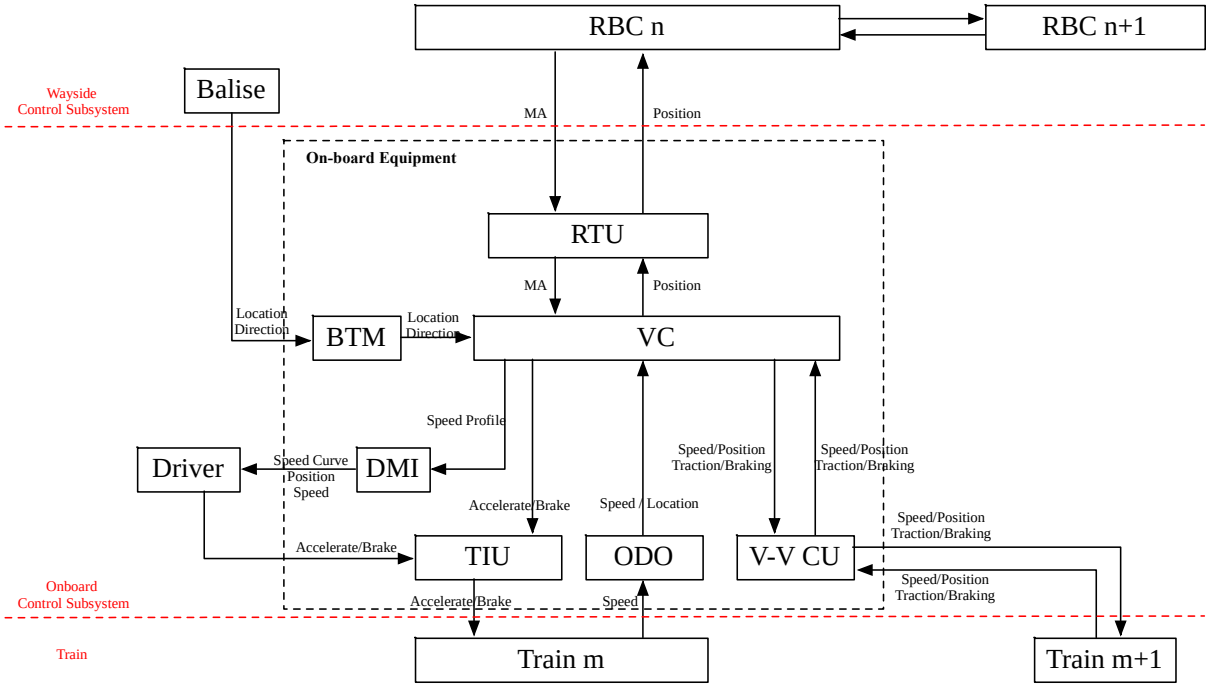

Figure 8: Hierarchical control structure of the 'closer running' or ETCS Level 4 (Authors, 2018)

In the case discussed here, a train convoy runs on plain line and the associated hierarchical structure is presented in Figure 9. The information flow within the structure is provided in Figure 10.

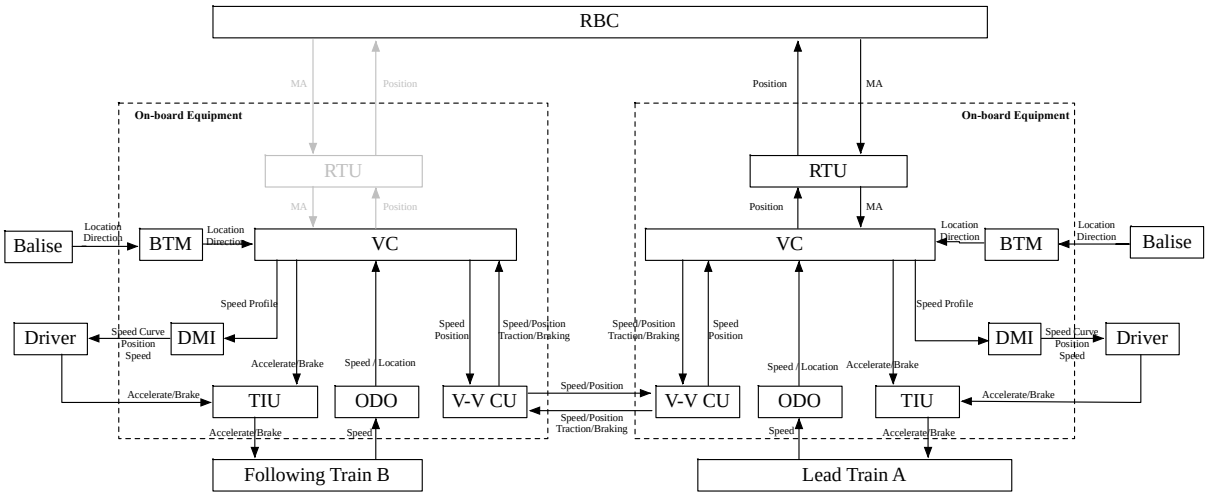

Figure 9: Hierarchical control structure for the scenario 'train convoy runs on plain line' (Authors, 2018)

The lead train A is controlled by ETCS Level 3. Therefore, train A communicates with the respective RBC to report its position and speed. Based on this information, the RBC generates an MA for the lead train A. The following train B is controlled by train A through the train-to-train communication unit that characterises 'ETCS Level 4'. The lead train A shares its speed, position, traction and braking rates with the following train B so that Train B can calculate its MA based on train A's status.

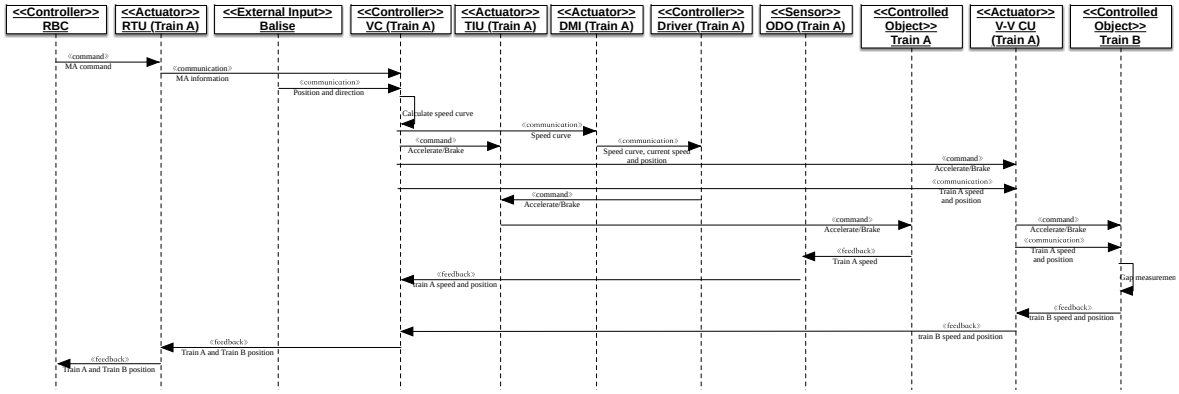

Figure 10: Information flow in the hierarchical control structure using the extended UML (Authors, 2018)

4.2.3 Unsafe Control Action Identification

After modelling, the next step is to identify unsafe control actions (UCA) that could lead to hazards. Here, the authors selected only Hazard 1 for analysis. From Figure 10, it is easy to extract commands sent by controllers. By associating these with the four types of unsafe control actions which are proposed by Leveson (2011b), the pathways to Hazard 1 are identified and are shown in Table 8.

Table 8: Unsafe control actions that lead to Hazard 1 (Authors, 2018)

Hazard 1: The following train (Train B) collides with the leading train (Train A) on plain line track					
Controller	**Control Action**	**Not providing causes hazard**	**Providing causes hazard**	**Too early / too late, wrong order causes hazard**	**Stopping too soon / applying for too long causes hazard**
VC (Train A)	Accelerate (to TIU)	UCA 1: Accelerate command is not provided to Train A when train B accelerates.	-	UCA 2:Accelerate command is provided too late to Train A.	UCA 3: Accelerate command stops too soon for Train A.
	Brake (to TIU)	-	UCA 4: Brake command is provided to train A when it is not needed.	-	-

4.2.4 Causal Scenario Identification and Safety Requirements Extraction

After identifying the unsafe control actions that lead to Hazard 1, the next step is to identify why the unsafe control action would happen and how to deal with the situation. Leveson (2011b) provides the causal factors to be considered in each part of the control loop. Therefore, for each unsafe control action, the first task is to find the control loop with the unsafe control action and then examine each part of the control loop to identify the causal scenarios that lead to it. Following this, mitigations or solutions can be proposed to solve the causal scenarios.

For UCA1 to UCA4, shown in Table 8, the related control loops and information flows are shown in Figure 8 and Figure 9, highlighted in red. For better traceability, the number of each causal scenario is identified by a CS-UCA number-sequence number. The safety requirement is identified as a SaR-CS number-sequence number. UCA1 is presented as an example. The process is described by Leveson (2011a) where she discusses the relationships between controllers, sensors, actuators and controlled objects.

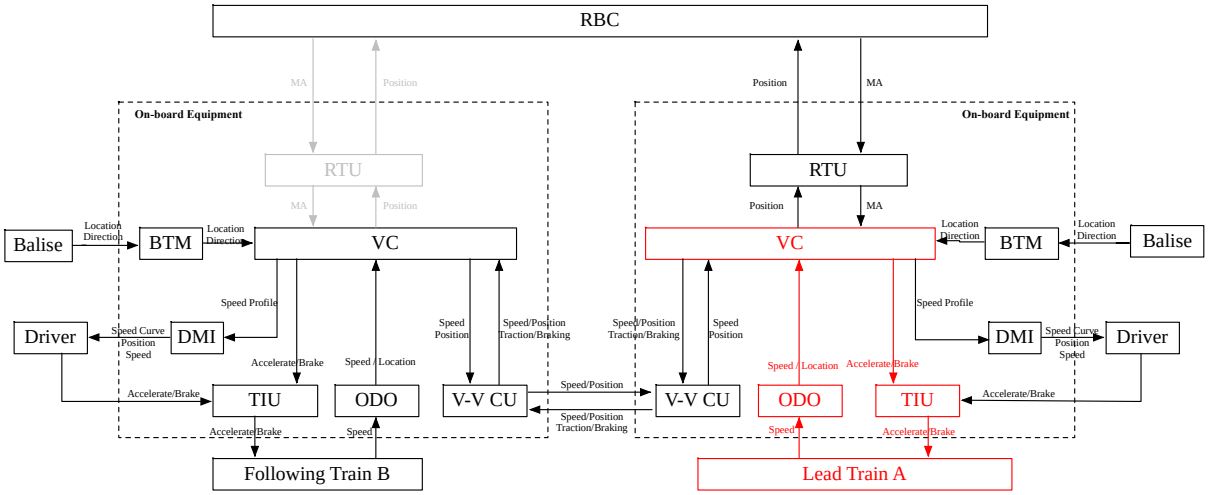

Figure 11: Control loops that are related to UCA 1 to UCA 4 (Authors, 2018)

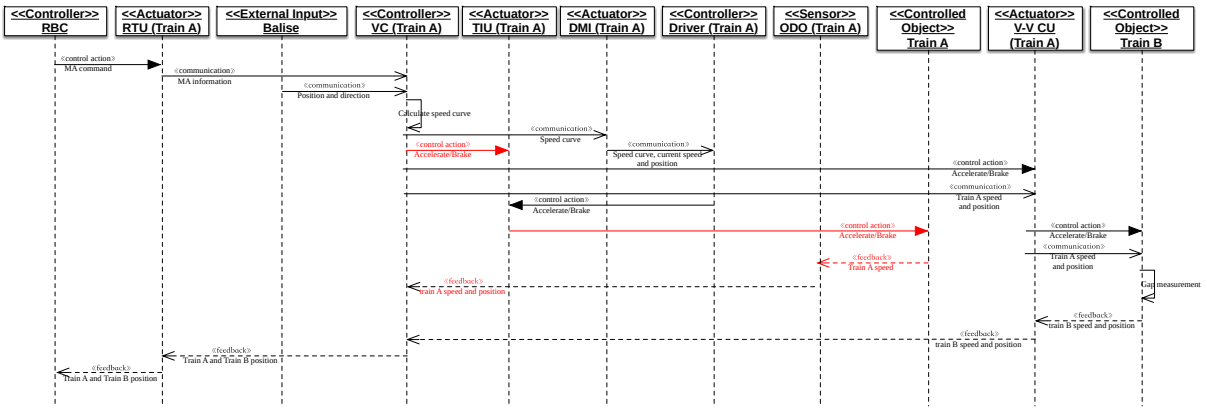

Figure 12: Information flows that are related to UCA 1 to UCA 4 (Authors, 2018)

Table 9: Example of causal scenario and safety requirement for UCA 1 (Authors, 2018)

UCA 1: The accelerate command is not provided to Train A when train B accelerates.	
Causal Scenario (CS)	CS1-1: TIU does not receive accelerate command from VC because of the communication between VC and TIU being broken.
Safety Requirement (SaR)	SaR 1-1-1: VC shall monitor train's acceleration. If it does not satisfy the standard acceleration, VC cuts down acceleration of following trains and report faults.
	SaR 1-1-2: VC shall monitor the communication with TIU. If it is interrupted, VC reports to driver and applies the emergency brake to all trains.
	SaR 1-1-3: Redundant communication line between VC and TIU.

Although approaches based on the STPA philosophy are often viewed as highly theoretical, our study shows that it can be applied to practical situations, such as the safety analysis of 'closer running' or 'ETCS Level 4'.

5 CONCLUSION

In this paper, we have presented two different methods for analysing the risk of implementing 'closer running' or the ETCS Level 4 concept, where trains follow each other at less than braking distance. The event tree analysis indicates that an individual passenger may be injured, due to a train stopping at an unacceptable rate, once in 1.23 million journeys. This falls into the region of negligible and, thus, tolerable risks from an individual perspective. However, at the network level, a catastrophic accident with multiple fatalities, indirectly caused by 'closer running' would result in very significant damage to the reputation of the railway and very high claims. Environmental factors present the greatest hazard that can lead to an unacceptable rate of deceleration. Climate change increases rainfall severity and thus increases the risk of landslides.

The authors have also presented an STPA based modelling approach that could be used to (i) identify hazards systematically and (ii) put in place appropriate defences or mitigations. Applying both methodologies together makes it possible to take informed decisions on the implementation of 'closer running' and the risks involved.

6 REFERENCES

Anna-Karin Lindberg, Sven Ove Hansson, Carl Rollenhagen, 2010. Learning from accidents – What more do we need to know?. *Safety Science,* 48(6), pp. 714-721.

BC, 2014. *Russia crash: Six dead in train crash near Moscow.* London: s.n.

Benner, L., 1975. Accident investigations: Multilinear events sequencing methods. *Journal of Safety Research,* 7(2), pp. 67-73 .

Emery, D., 2011. *Headways on High Speed Lines.* Lille, Union Internationale des Chemins de Fer.

ERA, 2016. *Memorandum of Understanding between the European Commission, the European Union Agency for Railways and the European rail sector associations.* Brussels: European Union Agency for Railways.

Eurostat, 2017. *Rail passenger transport, 2015 (passenger-km per inhabitant).* [Online] [Accessed 30 March 2019].

Health and Safety Executive (HSE), 2001. *Reducing Risks, Protecting People, HSE's decision-making process.* First Edition ed. Norwich, UK: Her Majesty's Stationery Office.

IEC, 2006. *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA).* 2 ed. Geneva: International Electrical Commission.

IEC, 2006. *Fault tree analysis (FTA).* 2 ed. Geneva: International Electrical Commission.

IEC, 2010. *IEC 65108, Functional Safety Standard.* 2.0 ed. Geneva, Switzerland: International Electrotechnical Commission.

IEC, 2016. *Hazard and operability studies (HAZOP studies) –Application guide.* 2.0 ed. Geneva: International Electrical Commission.

IRSE International Technical Committee, 2016. *ERTMS Level 4, Train Convoys or Virtual Coupling,* s.l.: s.n.

Leveson, N. G., 2002. *System Safety Engineering: Back To The Future.* Cambridge, Massachusetts: Aeronautics and Astronautics.

Leveson, N. G., 2004. A New Accident Model for Engineering Safer Systems. *Safety Science,* 42(4), pp. 237-270.

Leveson, N. G., 2011a. *Engineering a Safer World: Systems Thinking Applied to Safety.* 1 ed. London: Masa.

Leveson, N. G., 2011b. Applying Systems Thinking to Analyze and Learn from Events. *Safety Science,* 49(1), pp. 55-64.

Lindberg, A., Hansson, S. & Rollenhagen, C., 2010. *Learning from accidents - what more do we need to know.* s.l.:Elsevier.

M&EE, 2015. *Code of Practice for Brake Testing of Road Rail Vehicles.* s.l.:s.n.

ORR, 2019. *Passenger train kilometres by operator - Table 12.13 (Source: Network Rail).* [Online] Available at: https://dataportal.orr.gov.uk/displayreport/report/html/5410796f-c38d-49b9-9518-8297ec86f1ca [Accessed 4 April 2019].

RAIB, 2007. *Collision between a train and a road vehicle, M20 overline bridge, Aylesford5 February 2007,* London: Department for Transport, Rail Accident Investigation Branch.

RAIB, 2008. *Collision of a train with a demolished footbridge, Barrow upon Soar, 1 February 2008,* London: Railway Accident Investigation Branch, Department for Transport.

RAIB, 2011. *Derailment in Summit tunnel, near Todmorden, West Yorkshire (Page 13),* London: UK Department for Transport, Accident Investigation Branch.

RSSB, 2001. *Railway Group Standard GM/RT2044.* London: RSSB.

RSSB, 2006. *GRAIL: GNSS Introduction in the RAIL sector: WP1: Service Enabler Analysis.* London: RSSB.

RSSB, 2016. *GM/RT2045 Compatibility Requirements for Braking Systems of Rail Vehicles.* London: RSSB.

RSSB, 2017. *Annual safety performance report 2015-2016 RSSB,* London: Rail Safety and Standards Board.

RSSB, 2017. *Closer running (reducing headways): RSSB Research Report T1095,* London: RSSB.

Smith, D., 2011. *Reliability, Maintainability and Risk.* 8th ed. Oxford: Butterworth-Heinemann .

UK SI 1992, 2005. *The Railways (Accident Investigation and Reporting) Regulations 2005,* London: UK Government.

UNISIG, 2016. *ERTMS / ETCS Safety Requirements for the Technical Interoperability of ETCS in Levels (Subset-091, Issue: 3.6.0).* 3.4.0 ed. Bruxelles: UNIFE / UNISIG.

Williams, C., 2016. *The next ETCS Level?.* s.l., 2016 IEEE International Conference on Intelligent Rail Transportation (ICIRT) .

Winter, P., 2009. *Compendium on ERTMS: European Rail Traffic Management System.* 1 ed. Hamburg: Eurail Press.

APPENDIX: OVERVIEW OF SOME ACCIDENTS CAUSED BY OBSTRUCTIONS

Table 10: Two of five Examples of Occurrences of Payloads falling from Trains 2006-2016

Location	Date	Details	Consequence
Cricklewood curve	31/01/2006	Embankment slip led to track twist which caused wagons to overturn.	Wagons fell clear of track but could have fallen onto adjacent lines.
Scout Green, Cumbria	07/03/2015	Container detached and fell down embankment.	Operational disturbance.

Table 11: Two out of seven Occurrences of failed Infrastructure fouling Lines 2006-2016

Location	Date	Details	Consequence
Cambridge	05/01/2012	Subsiding OLE mast caused pantograph to fail.	Damage to train.
Moston, Manchester	28/01/2015	Passenger train collided with damaged platform.	Train damaged.