MSc in Railway Systems Engineering and Integration

College of Engineering, School of Civil Engineering

University of Birmingham

Configuration Management in Safety Critical Systems - Case studies Santiago de Compostela train derailment and LUL train departed with doors open incident

Author: MUHAMMET KANDEMIR

Date: 01/09/2014

Supervisors: BRUCE ELLIOTT and FELIX SCHMID

Dissertation submitted in partial fulfilment of the requirements for the award of MSc in Railway Systems Engineering & Integration

Executive Summary

Railways are complex systems and not easy to manage and control. With the developing technologies, it is almost inevitable to make changes on railways and these changes may bring risks with themselves. So it is crucial to do necessary assessment before implementation of a change. Also in order to provide safety in organisations, information about the changes should convey to the people who will take over the responsibility. It is common to see deadly accidents on the news and some of them might have been prevented thanks to proper configuration management (CM).

In this project, there are two case studies which are accidents. So in order to understand how accidents happened two popular accident causation models were reviewed with their criticisms in the literature review. One of them is Reason's model which is based on "Swiss cheese" model and second one is Leveson's model which is based on constraints. These models help to see relation between causes and effects (Qureshi, 2008). Also definition of CM and criticism of the yellow book (RSSB, 2007) were mentioned in the literature review chapter.

The aim of this project is to seek answer for the question (can better configuration management prevent accidents?). One of the case study in this project is the Santiago train derailment which resulted with 79 people were killed and around 140 people were injured. The author was advised by Mr Felix Schmid that before the Santiago accident happened there were probably some deficiencies in CM in the organisation. Therefore it was chosen for a case study in this project.

The other case study is London Underground Limited (LUL) open door incident which happened due to confusion of the driver. Fortunately, no one was hurt during the incident and the train was taken out of service after the incident. It can be seen from the incident report that one of the main causes of the incident was the sensitive edge system override modification. It is also mentioned on the report that LUL had not done necessary risk assessment before implementation of the change. Proper CM required to do necessary risk assessment and to be sure that the change is necessary and results of it acceptable. So it was thought that the LUL incident would also have been prevented thanks to proper CM.

In order to review whether the organisations did proper CM, a checklist was generated by using the document -ISO 10007:2003 Quality management systems-. The checklist consisted of two parts; organisational and change parts. Then by using data from internet and official documents, the probable causes of the incident and accident were listed. Also Reason's and Leveson's accident causation modes were simply applied to the case studies. After that the checklists were filled by drawing upon on the information and the data, and

then the deficiencies in CM were found. The deficiencies were mentioned with their explanations in this project.

The deficiencies were matched with the probable causes of the accidents. It showed that some of the main causes of the cases are related to the deficiencies. It was concluded that if proper CM had been done before the accidents, the deficiencies would not have existed, so some of the main causes of the cases would have been resolved thanks to proper CM. So if proper CM had been done, the accidents would have been prevented.

It can be concluded that proper CM may prevent some future accidents and so why not every organisation does not do proper CM. However doing proper CM may require extra budged and extra stuff. Its requirements may be difficult to comply with for some organisation, so organisations should review CM option before doing it and they should do proper CM. Otherwise it may not help to prevent accidents and it may just be extra budged for the organisations. Investing money on safety prevents potential accidents and accidents mean losses for organisations. Therefore investing money on CM does not mean dead investment, it rather means saving money and reputation.

Organisations think that they are enough safe otherwise they would take precautions. So they cannot easily foresee potential accidents ant do not put precautions to prevent future accidents. However proper CM helps to see risks on organisations and prevent organisations from bad decisions. Accidents harm organisations in terms of losses, bad impression, and damage cost. It means if potential accidents are prevented, organisations will not lose money and their popularity above all they may save lives.

The author thinks that safety is important and importance of the safety should be comprehended by the every people in organisations because those people maintain safety in organisation. Systems and constraints enforce people to provide safety without participation of people, safety may not properly is provided. CM may prevent some critical accidents but even CM is implemented by people, so training of the people is highly important for providing safety.

Table of Contents

List of Figures

List of Tables

Glossary of Terms / List of Abbreviations

Term	Explanation / Meaning / Definition
ASFA	Automatic Braking and Announcement of Signals
ATP	Automatic Train Protection System
BR	British Rail
CIAF	Comisión de Investigación de Accidentes Ferroviarios
CM	Configuration Management
CSA	Configuration Status Accounting
DMI	Driver Machine Interface
ERTMS	European Rail Traffic Management System
GB	Great Britain (England, Scotland and Wales)
ISO	International Organization for Standardization
LEU	Line side Electronic Unit
LUL	London Underground Limited
MS	Microsoft
NR	Network Rail
RSSB	Rail Safety and Standards Board
SPAD	Signal Passed At Danger
STAMP	System-Theoretic Accident Model and Process
TCDD	Turkish state railways
TCMS	Train Control Management System
TLA	Three Letter Acronym
UIC	International Union of Railways
UK	United Kingdom (Great Britain and Northern Ireland)

1 Introduction

Railways are complex organisations and have more than one stakeholder, so managing railways needs professional management systems. There can always be mistakes and failures in every organisation and these can sometimes end with deaths and injuries. No organisation wants their systems failures or employee mistakes to end up with injuries and deaths. Accidents in organisations also lead to acquiring a bad reputation. Therefore organisations invest huge amounts of money to improve safety. Investment does not always mean organisations and systems are safe, because management of organisation affects whole system safety. In organisations a mistake of one person may not lead accident but when human mistakes and system failures meet at the same point, they may cause an accident. In order to prevent accidents, there are usually mitigations, in other word extra layers, to protect systems from accidents. Despite these precautions, mistakes and failures may pass through layers and these can lead to accidents. Some properly unplanned changes may cause catastrophe or incidents. Configuration management (CM) helps to control changes and risks in organisations.

A LUL train travelled with doors open on the Victoria line on 11 July 2011. The driver could not deal with the sensitive edge system and he did not close the doors before departing from the Warren Street station. There was a change on the sensitive edge override system and it misled the driver. Also the Santiago de Compostela train crash was an accident involving death as well as many injured passengers and there are some evidences that it might be prevented thanks to proper CM. At first glance, it looks that the accident and incident happened due to the drivers` mistakes. However mankind have potential to make mistakes, so systems usually do not just rely on human care, they have also other protection systems.

1.1 Aims & Objectives

In this dissertation, the author tried find an answer to the question (Can proper CM prevent accidents). Also as case studies, the LUL train open doors incident and the Santiago de Compostela train accident and were reviewed in terms of CM. It is aimed to see if proper CM had been done, would the accidents have prevented?

1.2 Scope

By drawing upon on the document "ISO 10007:2003, Quality management systems - Guidelines for configuration management" the checklist were generated and they helped to see how well the organisations complied with CM before the accidents happened. This project includes the probable causes of the accident and the incident, and also includes basic application of two accident causation models (Reason's and Leveson's models) into the case studies. This project also illustrates how the checklist was prepared and it shows how the checklists were used to review CM in the organisations.

1.3 Methodology

The dissertation is basically about configuration management on railways. The LUL train open doors incident happened in 2011 and an incident report was released in 2012. So the necessary information was taken from the report. However the train derailment in Spain happened last year and investigations are still being conducted by CIAF (Puente, 2013). Therefore the information and data about the accidents are not from directly primary data. Most of the data in this project are secondary data which were collected from articles, webpages, journals and books. Also some information and data were collected from discussion groups on the website (www.linkedin.com). The group members are generally professional in the area of railway and the information they share is usually from primary sources.

Accident causation models provide better understanding of causes and effects relations, so two common accident causation models; Reason’s and Leveson’s models were reviewed in the literature review. The models were compared to each other and criticisms about them were mentioned. One of the good guidance for CM is the yellow book also criticised and definitions of the CM from different sources were mentioned.

The checklist was created directly using the document “ISO 10007:2003, Quality management systems - Guidelines for configuration management”. The document “ISO 10007:2003” provides guidance to implement proper configuration management within organisations. CM standards can be applied for products from concept to disposal (ISO, 2003). The preparation of the checklist was explained on the chapter 4.

In order to show connection between this project and its objectives, a flowchart diagram is used and it illustrates the solution of the problem. The following diagram below is the flowchart and it also shows the method.

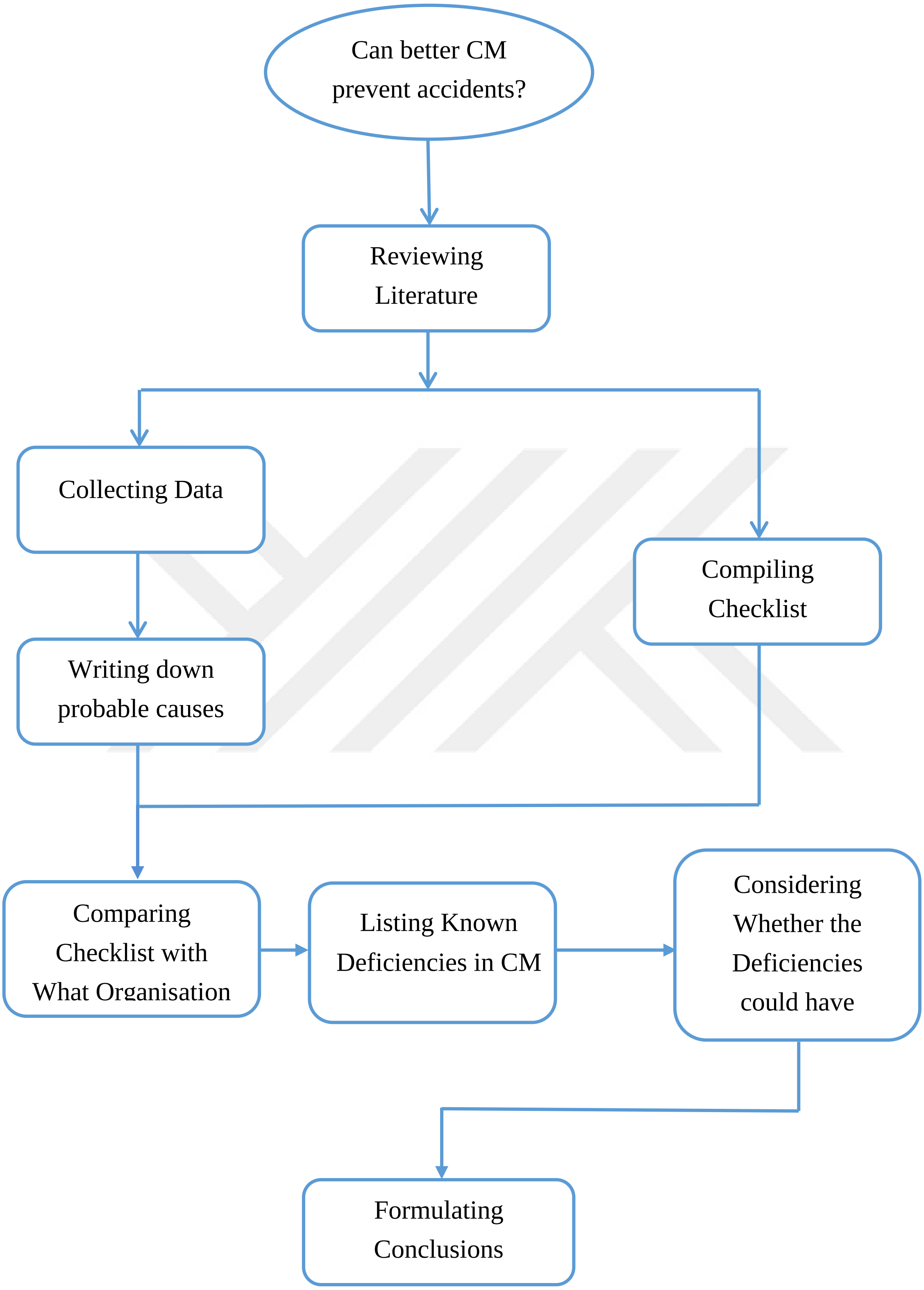

Can better CM prevent accidents?
Reviewing Literature
Collecting Data
Compiling Checklist
Writing down probable causes
Comparing Checklist with What Organisation
Listing Known Deficiencies in CM
Considering Whether the Deficiencies could have
Formulating Conclusions

Figure 1the flowchart of methodology (the author)

The main question is “Can better CM prevent accidents on railways?” Therefore the question/problem is at the top of the flowchart. In order to understand proper configuration management and its implementation on railways, The **yellow book** (Engineering Safety Management book) is a very useful guidance and the (ISO, 2003) standards are quite advantageous to implement on organisations. These sources were used to generate the checklist.

Then the dissertation splits into two branches, one of them is preparing a checklist and other is to collect data about the accidents.

- Preparing a checklist: The check list also was slit up into two parts which are organisational and change parts, because more than one change might be done in the same organisation.
- Collecting data: Most of the data and information about the accident was collected from websites and jurnals. By using the data, probable causes contributed the accident are detected and listed in this project.

Afterwards in the light of data and information, the checklist was filled in by the author. As a result of the checklist, the deficiencies in CM were discovered. After finding the deficiencies in CM, the deficiencies and the probable causes were matched to see whether proper CM would have prevented the accidents. Then how proper CM would have prevented the accident was explained.

1.4 Dissertation Structure

This dissertation project consists of 10 chapters and the chapters are briefly explained below. The first chapter is introduction, so it was not presented below. The other chapters are as follows:

- Chapter 2 includes background and it gives basic information about the accidents for example; general information about Spain train accident in 2013, general information about automatic train protection system and information about ERTMS.
- Chapter 3 includes the literature review and it consists of briefly definition and explanation of configuration management mostly based on `The Yellow Book`. Also it includes Reason’s and Leveson’s accident causation models with discussion about them.
- Chapter 4 includes definition of the checklist, preparation of the checklist and implementation of the checklist on the organisations. This chapter also includes some answer such as why the author chose the checklist method to evaluate CM in those organisations.

- Chapter 5 includes the case study “Train departed with doors open, Victoria line, LUL” In this chapter; event sequence of the incident was explained. Also probable causes of the incident were listed and by using the primary data (incident report), CM deficiencies were found by the author. A basic application of the Reason’s and Leveson’s models were presented in this chapter.
- Chapter 6 includes the case study. The case study is main part of this project and about Santiago de Compostela train derailment. In this chapter, event sequence of the derailment was explained. Also probable causes were listed and by using the secondary data about the accident, CM deficiencies were found by the author. A basic application of the Reason’s and Leveson’s models were presented in this chapter.
- Chapter 7 gives answer to main question (Could proper configuration management prevent the accidents) of this dissertation.
- Chapter 8 includes total conclusion of this dissertation. The conclusion consists of findings, recommendations, review of approach and areas for further research.

2 Background

2.1 LUL train incident

The LUL train incident was explained in the chapter 5, so it was not explained here again. In this chapter, technical information about the LUL train incident was given. In the chapter 5, sensitive edge system, driving modes and train control management system were not deeply explained, so it may look quite complicated. It is recommended to read background section before reading the chapter 5.

2.1.1 Sensitive edge system

The sensitive edge system is activated when an object traps between train doors. The system open the doors by 25 mm to 75 mm, and then the doors stay open for 0.5 seconds before re-closing when the doors an counter an obstacle. If the obstacle still remains after first attempt of closing doors, the system make two further attempts. After third attempt, if the obstacle still remains, the train will not be obtained traction power. If the all doors of train are closed, the operator can get traction power, otherwise it is not possible. The sensitive edge system works by parallel conductors in the vertically placed rubbers of the train doors (RAIB, 2012).

2.1.2 Driving modes

The train have three types of driving modes (RAIB, 2012):

- Automatic: when the driver presses two starts button the mode is activated, the system accelerates, brakes, and stops the train as required. This also called normal mode in passenger service. ATP prevents the train from colliding.
- Protected manual: in this mode normally used in the limit of the depot and the speed limit is 80 km/h for this mode. ATP also prevents the train from colliding.
- Restricted manual: this mode is similar to protected mode apart from speed limit. Maximum permitted speed is 16 km/h in this mode.

2.1.3 Train control management system (TCMS)

The system monitors, displays, and records faults and things related to the train electrical and electronic system. It is a computer system on-train. The TCMS provides interface with train driver via a touch screen in the driving cab. Thanks to the screen, the operator can see the data which provided by TCMS.

TCMS message lead the train drivers about technical actions need to be taken and gives information about the train’s condition. The messages are display with an audible alarm and the train driver must acknowledge. When cause of the message with alarm is solved, the driver can delete the message by the button on the touch screen (RAIB, 2012).

2.2 Santiago train accident

In Spain, railways are operating by state owned company Renfe which is under the ministry of development. Renfe is responsible for operating passenger trains, freights, train leasing and rolling stock maintenance in Spain (Railway Gazette, 2013). According to "**EU Directive 91/440**", Renfe was divided into Adif and Renfe operations. Railway infrastructure administrator (Adif) is almost managing all railway networks of Spain. Adif is responsible for maintenance of existing networks and constructing of new networks in Spain. Adif is funding by Spanish government (Spain Ministry of Development, 2014).

2.2.1 Madrid – Galicia line

According to (Adif, 2012), the Madrid – Galicia line is built with double electrified track and with the speed up to 350 km/h. The route between Madrid-Valladolid Line in Olmedo and Santiago de Compostela is 434.86 km long with ERTMS ETCS level 1 and ASFA signalling (ERTMS ETCS Level 1 and ASFA signalling are identified on the Background chapter). ERTMS and ASFA are train protection systems and ASFA is Spanish train protection system. The important point about the train protection systems is that the route was equipped with ERTMS until 4 km before the accident site and the accident site was just equipped with ASFA. So the accident happened on the track which is just equipped with ASFA signalling. The following map helps to understand locations of the cities.

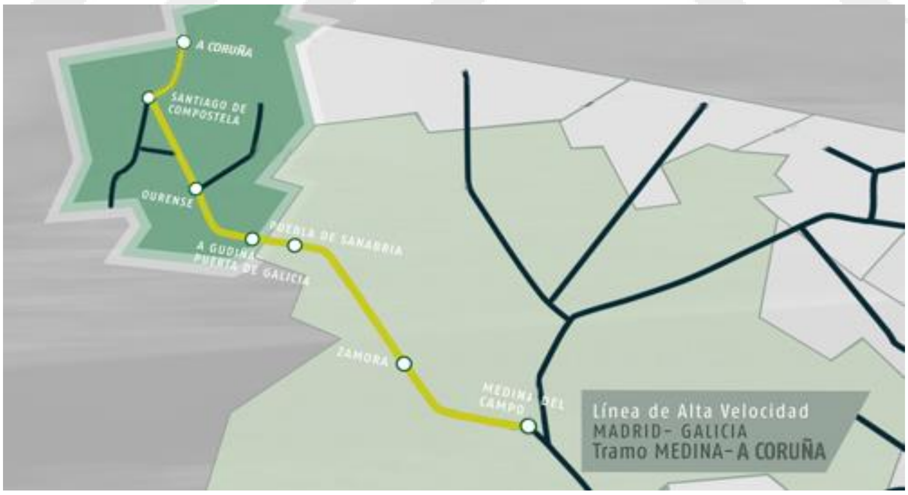


Figure 2 Madrid - Galicia line map (www.adif.es)

The (Adif, 2012) announced that the Ourense – Santiago route connects the Northwest with the Centre and North of the Spanish peninsula, so it is important route. Thanks to new line, the journey time between Ourense and Santiago de Compostela is reduced from 1 hour 34 minutes to 38 minutes. This part of the route includes a total of 38 viaducts and 31 tunnels which shows the difficulty of the route. The new line is also reduced the conventional line by 39 km.

2.2.2 The crash site

The accident happened just after the last tunnel before the Santiago de Compostela station. As mentioned above there are 31 tunnels on the route between Ourense and Santiago de Compostela. In addition after the last tunnel a tight curve starts and speed limit is 80 km/h while speed limit is 200 km/h just before the curve on the route (Sky News, 2013).

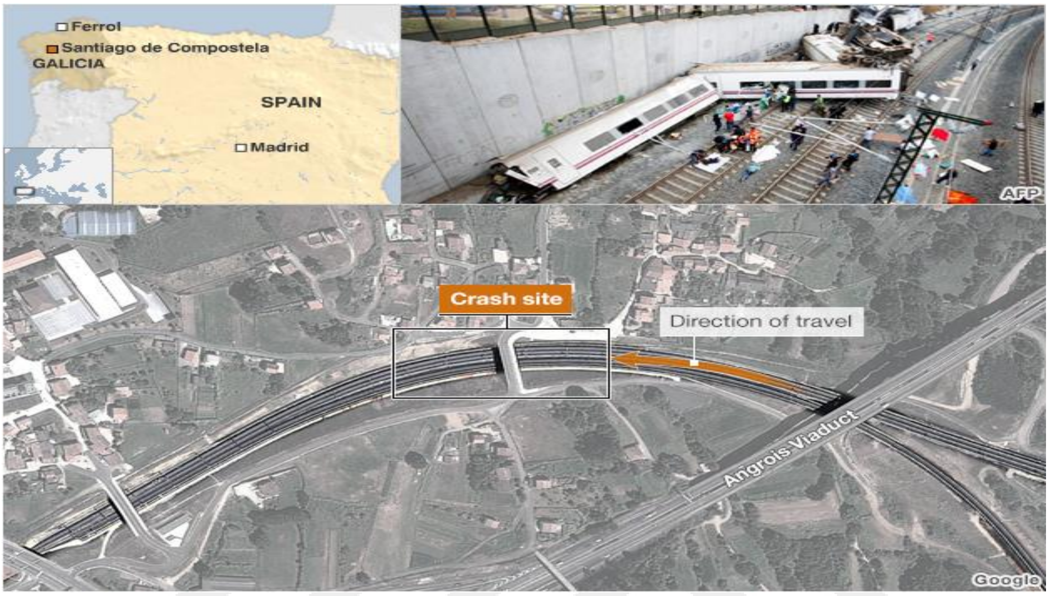


Figure 3 scene of the accident (www.bbc.co.uk)

The figure 3 illustrates the crash site and the picture on the figure above taken just after the crash. It can be seen from the figure 3 that there are double track high speed line and a single conventional track. The accident happened on the high speed line and an arrow shows the direction of train on the figure 3. The curve is 3 to 4 km from the Santiago de Compostela station. The high speed line between Ourense and Santiago de Compostela follows the same route with the conventional line from the curve to Santiago station. The curve was equipped with the Spanish train protection system – also known as ASFA. 4 km before the curve, the route is equipped with ETCS level 1 signalling system and the train also is equipped with ETCS on-board equipment, but there is no communication between ASFA signalling and ETCS on-board equipment (BBC & Westcott, 2013).

The ASFA signalling system on the line warns drivers when they go faster than the speed limits, but the balises on the curve does not interfere up to 200 km/h speed. The ASFA prevents the trains from going faster than 200 km/h on the curve (ERTMSnews, 2013). ERTMS ETCS level 1 was equipped until 4 km before the accident site and it used for a certain time, but at the transition point between ASFA and ERTMS, it caused delays. So about nine months before the Santiago accident, Renfe asked the drivers to switch off ETCS on driver’s cab, because it used to cause delays (ERTMSnews, 2013).

When ETCS is switched on the driver's cab, the drivers have to slow down and acknowledge ETCS that they are aware of switching the signalling systems at the transition point on the Santiago line. So the drivers used to know when they switch the signalling systems and approach the tight curve where the accident happened. At least thanks to the transition point, the drivers act more careful than the situation when the accident happened. Because, without the transition point the drivers may not remember the actual position of the trains and may make mistake due to confusion. The driver said that "he believed he was in the other section of the road" (ELPAIS, 2013).

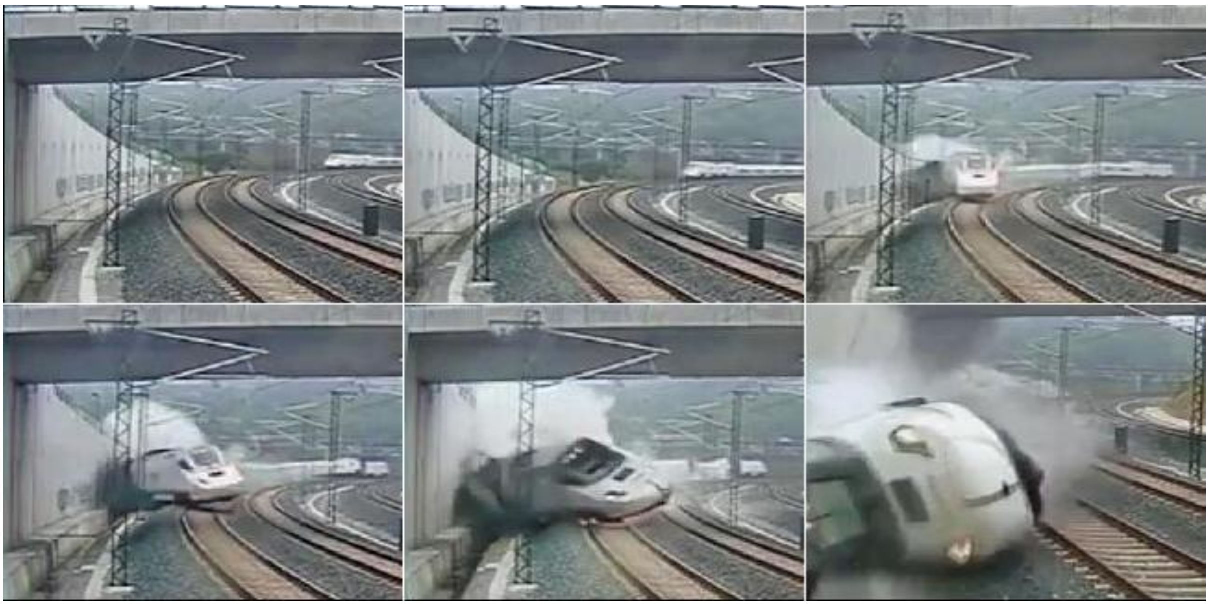


Figure 4 the video footages of derailment (theaustrailian.com.au)

The video footages above show that firstly the passenger coaches are located between two locomotives at the each end came off tracks and then locomotives. Due to high speed on curve one of the carriages flung on the embankment wall. The train Alvia 730 series can run electrified and non-electrified lines thanks to its diesel engines on locomotives. However extra features do not mean advantage always, it could be disadvantage sometimes which it would be very big disaster if one of locomotives exploded. Even none of locomotives exploded, the locomotive at the end caught fire after train derailed. The train had **2** locomotives and **8** carriages and **1** buffet car totally **11** units and it is **183** m length and **354** tonnes weight. It has ability to travel at top speeds of **250** km/h (UIC gauge). It is also able to run on to different track gauges (Talgo, 2013).

2.3 Automatic Train Protection system

The author chose the Australian definition of the automatic train protection system (ATP) because it is easy to understand and helps to readers to understand it quickly. The (Transport for NSW, 2011) explains that ATP is installed to prevent trains from going too fast and SPAD. It is a safety system and reduces railway accidents substantially. ATP requires on-train and track side equipment in order to identify unsecured conditions. Depends on situation, it can slow train or stop train as well as it warns driver via on-train equipment if it is necessary. There are four main features of ATP which are:

- Inform drivers beforehand about the route ahead
- Execute route speed limits
- Prevent trains from SPAD
- Prevent drivers from going too fast when ahead signal is at stop

2.3.1 ATP trackside equipment

The trackside equipment is Lineside Electronic Units (LEU), transponders. The LEU receives information about route, speed limits, signal, gradient and location then conveys the information to transponders. Although transponders can be balises, Euroloops and radio infill units, balises are quite popular (Transport for NSW, 2011).

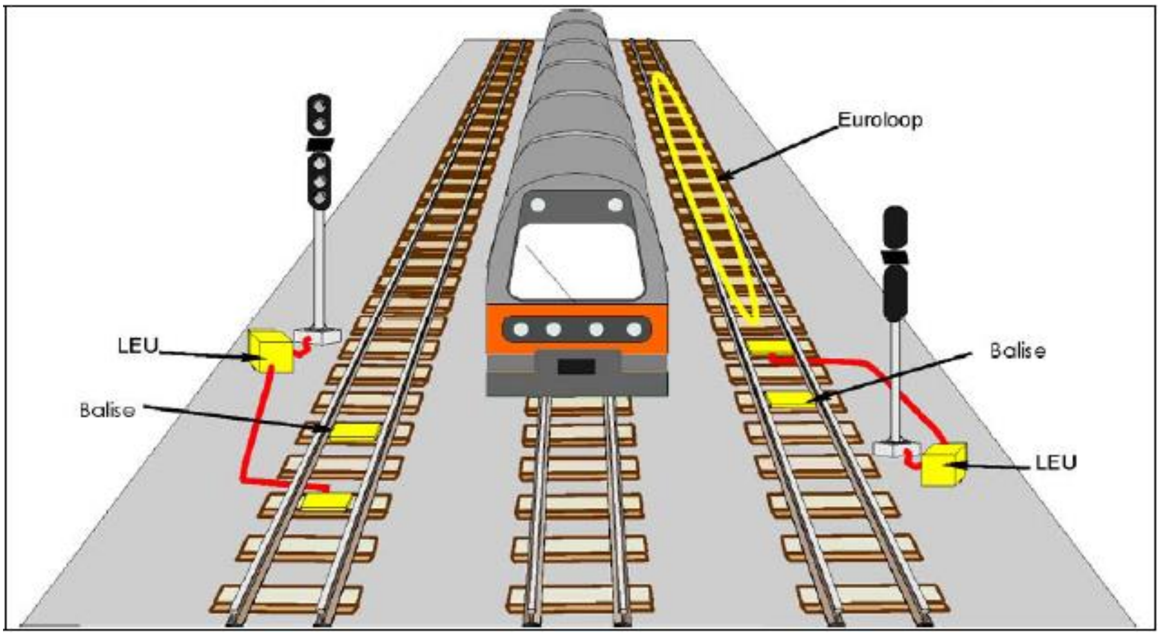


Figure 5 ATP trackside equipment (Transport for NSW, 2011)

2.3.2 ATP on-board equipment

According to the (Transport for NSW, 2011) ATP on-board equipment:

- An antenna to receive signals from trackside transponders
- An on-board computer which process data from both track and train to give appropriate decision
- A Driver Machine Interface (DMI) which located in the drivers cab
- In order to measure travelled distance, an odometer
- An interact system to stimulate train brake systems.

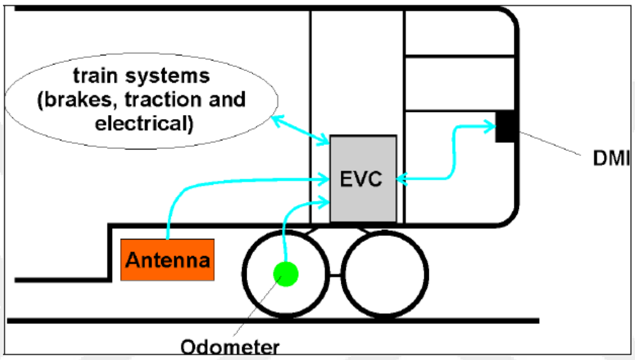


Figure 6 ATP on-board equipment (Transport for NSW, 2011)

2.3.3 Automatic Braking and Announcement of Signals (ASFA)

ASFA is widely used in Spain and it is a train protection system as well as cab-signalling. ASFA can transmit nine different data between track and train. Although it is not a fail-safe system, it can warn drivers as visual and audial if it is necessary. The driver must acknowledge restrictive signal within 3 seconds by pressing and releasing button on drivers cab. It stops train if the driver doesn't comply with the signal restriction or goes faster than speed limit on route (Connor, et al., 2014).

2.4 ERTMS ETCS Level 1

The advantage of ETCS level 1 is that is an existing signalling system. The trackside equipment of the system are LEU and Eurobalises. There is an electrically connection between balises and the signal or connection via LEU. The balises provide communication between LEU and on-board ETCS equipment. The signal aspect is transmitted from trackside signalling system to balises via LEU and the balises convey the signal aspect and route information, such as speed restriction and gradient, to train (RSSB, 2010).

An antenna, a part of ETCS on-board equipment on the train, picks up the data and ETCS on-board computer uses this data to calculate maximum speed and braking curve.

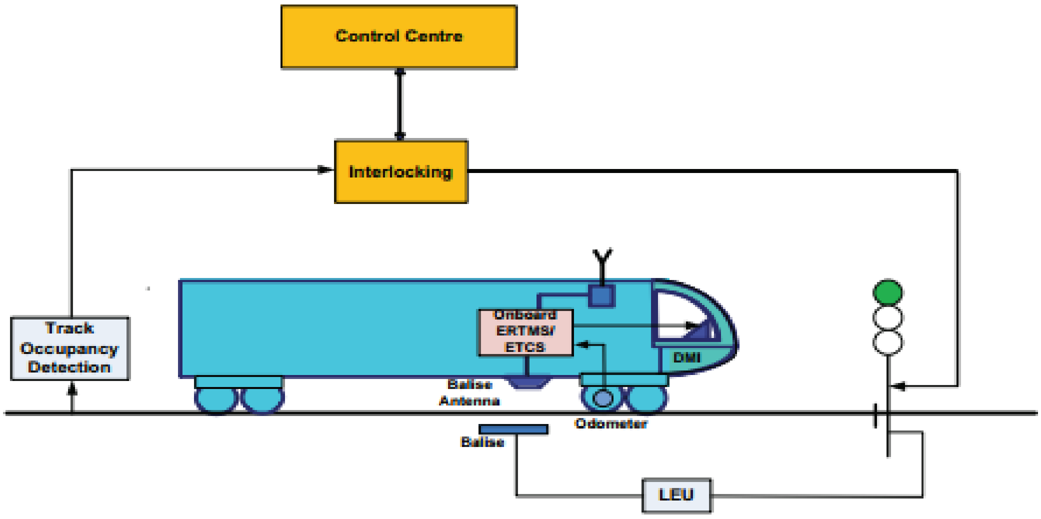


Figure 7 ERTMS level 1 application (Abed, 2010)

The ETCS level 1 also prevents trains from passing signal at danger and also from exceeding speed limit. The driver also has to follow trackside signal. The maximum speed, safe braking distance, braking curve are calculated by ETCS on-board computer. The control centre controls and checks the train and also manages interlocking (Abed, 2010).

3 Literature Review

3.1 Configuration management

There are some definitions of configuration management and they are given below.

The (ISO, 2003) definition is: “Configuration management is a management activity that applies technical and administrative direction over the life cycle of a product, its configuration items, and related product configuration information.”

The (RSSB, 2007) definition is: “A configuration is a group of related things and the relationships between them, and configuration management is about keeping track of these things and their relationships.”

The (Müller, 2013) definition is: “Configuration Management is an approach to control system configurations with dedicated engineering processes, methods and tools.”

The (EIA, 2004) definition is: “A process that establishes and maintains consistency of a product’s attributes with its requirements and product configuration information throughout the product’s life cycle.”

It can be seen from the CM definitions that they are similar. They all emphasize that it is control process which tracks a product with its relations throughout its life cycle.

The following section was written by drawing upon on the yellow book (RSSB, 2007). In order to provide safety, organisations should record every change and their relationships. Keeping records of them helps the organisations in following topics:

- Helps to see how the change was done and what have been done, so in the future the people who make changes, have information about former changes.
- By looking at the records, the organisations can say that they have reduced risk on an acceptable level. Also the organisations show the records to other persons
- It helps to handover safety responsibilities to other people

One of the functions of configuration management is to provide accuracy between “information world” and “real life”. In other words, it helps organisations to do what they have planned. Otherwise the organisations may not show a proof that they properly provide safety.

The yellow book mentions benefits of proper CM and they introduce above, however the author thinks proper CM has benefits more than mentioned in the yellow book. Because CM requires organisations to make planned, described and evaluated change besides keeping track of changes and relationships. CM helps to control changes and it also helps to protect systems. The yellow book does not mentioned how CM prevent accidents, although preventing accidents is an important benefit of proper CM. The yellow book is a guidance and gives suggestions about implementation of CM, however it is not sufficient to encourage organisations to do CM. Organisations would like to invest money on things which make noticeable effect on organisations like ATP. Therefore if organisations are not informed about how CM prevent accidents, they do not interest in doing CM.

3.2 Accident causation models

In this section, two of the common accident causation models; Reason's and Leveson's models, were explained. Accident causation models help to understand how accidents happened and relations between causes and effects (Qureshi, 2008). They are very useful to explain accidents to readers. They also encourage organisations to see deficiencies in the organisation and to put precautions to prevent potential accidents.

3.2.1 Reason's model

This section is based on the book (Reason, 1997) and the report (University of Aberdeen, 2003). As it can be seen from the figure 8 that hazards pass through defences/barriers by using the holes on the defences. The purpose of the defences is to prevent accidents, but defences have random holes on itself. Reason categorises factors which contributes accidents. The factors are unsafe acts, local workplace factors and organisational factor and these were explained on the following paragraphs. The report (Elliott, et al., 2012), explains that the model moves from blaming human errors to the environment in which human works.

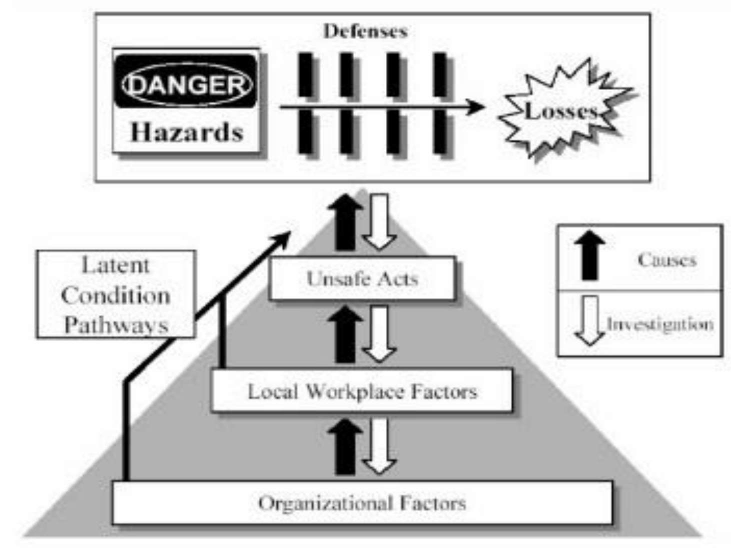


Figure 8 Swiss cheese model (Reason, 1997)

Organisational factors

Organisational factors may be described as the way of doing things and behaviour of people in the organisation. Developing the cultural factors take long time in an organisation. Because changing, wide spreading and being stimulated of the cultural factors is slow. External factors like politic and economic factors have very important effects on high-level decisions. Organisational factor can be exampled as: Strategic decisions, managing, generic organisational processes, auditing, forecasting, allocating resources, budgeting, planning, scheduling, communicating and like.

Local workplace factors

Local workplace factors affect performance and effectiveness of the people who works there. Whenever the workers do the core business, they are close to the potential local hazards. The negative effects of high-level decisions are conveyed via various department and organisation to the workplaces. The commission of unsafe acts is promoted by the local workplace factors. People in workplaces have potential to do unsafe acts. However usually only a few unsafe acts can make holes on the barriers and lead the damages. There are two main interacting local condition groups which are first group related to the task and second group related to mental and physical states of the works. As an examples of local conditions: time pressure, poor human-machine interface, inadequate tools and equipment, insufficient training, low pay, poor communications, unworkable procedures, under-manning and like.

Unsafe acts

When people's tendencies to make mistakes combine with the local working factors, *unsafe acts* happen. Usually front-line people have potential to commit unsafe acts and unsafe acts can be made by individuals or groups. Unsafe acts occur lots of time but not all of them make holes on the defences and result with damages.

Defences

Aim of the defences is to protect the system, remove and mitigate organisational hazards. They use majority of resources in an organisation when the organisation involves in dangerous activities. Defences are various and spread through the organisation, so it is very difficult to distinguish differences between non-defensive and defensive parts of a system. Failures generally happen in workplaces or on the defences. Mr Reason listed the aims of all defences in his book as:

- *To create* ***understanding*** *and* ***awareness*** *of the local hazards*
- *To give clear* ***guidance*** *on how to operate safely*
- *To provide* ***alarms*** *and* ***warnings*** *when danger is imminent*
- *To* ***restore*** *the system to a safe state in an off-normal situation*
- *To* ***interpose*** *safety barriers between the hazards and the potential losses*
- *To* ***contain*** *and eliminate the hazards should they escape this barrier*
- *To provide the means of* ***escape*** *and* ***rescue*** *should hazard containment fail.*

According to the Reason there are two types of failures *active* and *latent*. The failures in the workplace are usually related to *active* failures and *latent* conditions usually occur due to absence or lack of defences. Latent conditions are unavoidable in an organisation.

Criticisms of the Reason's model

Reason's accident causation model is very famous, so there are so many positive and negative views about it. Leveson's critics were given in other section (see 3.2.3). Three important critics about the Swiss cheese model:

The (Shappell & Wiegmann, 2000) says that:

The Reason's accident causation model has changed the general view of accident causation in many aspects. However, `swiss cheese` model is a theory and it also includes explanation of how to apply it in a real environment. Unfortunately, the theory does not explain meaning of the holes in Swiss cheese within everyday operations.

The (Luxhøj & Kauffeld, 2003) notes that:

One of the disadvantages of the Reason model is that it does not account for the detailed interrelationships among causal factors. Without these distinct linkages, the results are too vague to be of significant practical use.

The (Dekker, 2002) mentioned that:

The defences on the Swiss cheese model are not stable, and they are depended each other. They can support and interact each other. The model's analogy helps to see complexity of failures and to think about exertion to maintain safety of system. *But analogy itself does not explain:*

- *Where the holes are, or what they consist of.*
- *Why the holes are there in the first place.*
- *Why the holes change over time, both in size and location.*
- *How the holes get to line up to produce an accident.*

The author reviewed Reason's model with Leveson's model in the comparison section (see 3.2.1). So the review was not mentioned here.

3.2.2 Leveson's model (STAMP)

This section was written by drawing upon on the book (Leveson, 2011) and the thesis (Song, 2012). Most accident models rely on chain of events, although STAMP is grounded on system theory. In this model, constrains are basics concepts instead of events. Also inadequate control or implementation of safety-related constraint on the system conceives accidents. STAMP is based on three system theory concepts: safety constraints, safety hierarchical control, and process models (Leveson, et al., 2003).

Leveson compares assumptions about the cause of accidents in her book (Leveson, 2011) `engineering a safer world`. Reason's assumptions and Leveson's assumptions were listed above and they were taken from Leveson's book.

Reason's assumption 1: *Accidents are caused by chains of directly related events. We can understand accidents and assess risk by looking at the chain of events leading to the loss.*

Leveson's assumption 1: *Accidents are complex processes involving the entire socio-technical system. Traditional event-chain models cannot describe this process adequately.*

Reason's assumption 2: *Probabilistic risk analysis based on event chains is the best way to assess and communicate safety and risk information.*

Leveson's assumption 2: *Risk and safety may be best understood and communicated in ways other than probabilistic risk analysis.*

Safety Constraints

STAMP moved from focusing on events to constraints. Events only lead to accidents when constraints are not successfully enforced. In engineering, *passive controls* provide safety by existing of their presence and it can provide safety by a basic interlock system which limits interaction between components like containment vessels. For example: mechanic relays fault when contacts of the relays open. However *active controls* need action to provide safety. Leveson mentioned in her book (Leveson, 2011) that the following requirements are needed to provide active control.

- ***Detection:*** *hazardous event and condition*
- ***Measurement:*** *some variables*
- ***Diagnosis:*** *rendition of measurements*
- ***Response:*** *providing appropriate response*

Physical constraints limit the complexity on system design and in order to reach the goal, system-level constrains should be identified and they should be divided into groups to enforce by appropriate groups. Nowadays in order to provide the safety-level which is demanded by the society, first safety constrains should be identified and then effective controllers should be design to enforce them.

Hierarchical safety control

In hierarchy, in order to control processes at lower levels, control processes are operated between levels. Hierarchy structure illustrates relationships of different levels and also how the levels are controlled and what controls them. Some missing constraints may cause inadequate control at the levels of hierarchy structure.

In order STAMP to avoid from inadequate events, it uses enforcement of constraints in the system. Also it focuses on conditions rather than component failures. During the control processes, it is important to have effective communication channel between the levels of hierarchical structure. There are two types of communication channels showed figure below.

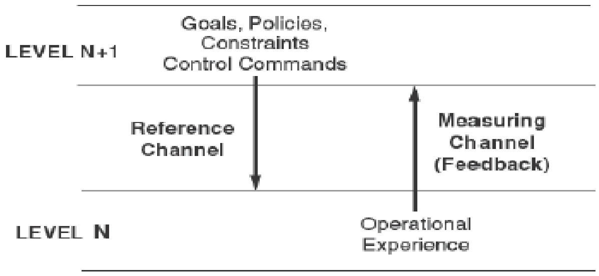

LEVEL N+1
Goals, Policies, Constraints Control Commands
Reference Channel
Measuring Channel (Feedback)
LEVEL N
Operational Experience

Figure 9 communication channels between control levels (Leveson, 2011)

The downward reference channel provides the information such as goals, policies, constraints and control commands to the level below. This information is important to impose safety constraints on the level which receives the information. The measuring channel gives feedback about the enforcement of safety constraints.

Process model

Process model is one of the concepts in STAMP and for controlling a process, four main requirements necessary:

- **Goal:** goal is enforcement of the safety constraints for STAMP.
- **Action:** implementation of the reference channel information.
- **Observability:** observation may be provided by sensors and with other ways and it is important for the operator to observe situation of the process.
- **Model:** any system needs a model of a process.

The process model helps to determine which control actions are required. The model is based on having information about current state of the controlled process and to predict the results of different control actions.

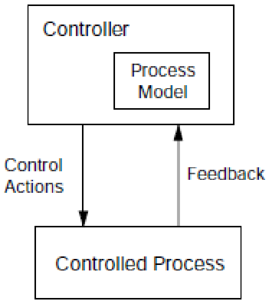


Figure 10 process model (Leveson, 2011)

The figure 11 above shows a general process model. Every controller should have a process model and the process model should match the system otherwise an accident can occur.

Accidents do not happen just due to component failures, but also interactions of system components. In this model, safety can be viewed as a control problem.

3.2.3 Comparison of these models

In order to prevent accidents, one of the best ways is to learn from accidents and understand why the accidents happened. So in this section, accident causation models were introduced. The models introduced this section have different approach to accidents, so it is thought that introducing two different opinions help to understand the models deeply. The first model is James reason’s model which is based on Swiss cheese model and the second model is Leveson’s model (STAMP) which is based on system theory and it focuses on constraints.

Leveson criticises Reason’s model that the model is simple to use but it is not useful for complex systems. Also it does not help to understand why accidents occur and how the accidents could be prevented.

Reason’s model alleges that accident are caused by chains of directly related events. However Leveson disagree with this idea and she says “accidents are complex processes involving the entire socio-technical system.” She also gives example that as a common impression, smoking causes lung cancer, but non-smokers also can be lung cancer and not every smoker is lung cancer.

Reason’s model supports probabilistic risk assessment arguing that passing of a hazard through the holes on the defences is very small probability according to the calculations. Leveson critises this idea due to each event is independently analysed in the probabilistic risk assessment. Leveson suggest that “Risk and safety may be best understood and communicated in ways other than probabilistic risk analysis.” The author agrees with the both models up to some point because each model has advantages and disadvantages. Reason`s model is simple and easy to use, but for complex accidents it may be insufficient.

These models are similar because both of them help to find main causes of accidents. However Leveson sceptically approaches accidents and seeks for all factors which contribute accidents as distinct from Reason’s model. Leveson’s model seeks for drastic solutions in order to prevent future accident and the model focuses on management and control failures. One of the editors of the yellow book Mr Elliott suggested that I should glance at the Clapham Junction accident, which is very important, because the accident forced British Rail (BR) to review itself because management factors also caused the accident besides technician mistake. The accident happened due to a loose and uninsulated cable which contacted to the rail and the signal turned to danger. The signalling wires had been renew and old cables had been left one side connected, so the loose cable contracted to the rail and caused to the passenger train stop on the route. Then another train which comes from same direction hit the passenger train and also an empty train from other direction hit the debris. As a result 35 passengers were killed and a lot of passengers were injured. The report of the accident was written by Mr Hidden and he presented very important recommendations to BR on the report (Hidden, 1989). The recommendations were about following topics:

- *Immediate cause of the accident*
- *Causes within management*
- *Improving BR's safety culture*
- *Mitigating the effects of any future accident*
- *Improving the response of the Emergency services*
- *Improving BR's response*

According to the Reason's model there are some defences which prevent accidents and in this accidents, the danger is, contacting of a loose wire and the defence is, insulating of loose wires. Therefore responsible person of the accident looks the technician who renews the cables (Hidden, 1989). However blaming the technician does not help to prevent future accidents, it just saves the day. The Hidden's report also shows that the technician had worked seven days a week previous thirteen weeks and an independent person had not inspected the work after completion of renewing project. For this accident Reason's model does not help to consider all the areas which recommended by Mr Hidden on the report. So it is not sufficient for complex accidents like the Clapham Junction accident.

4 The Checklist

A checklist is very useful tool for controlling assets, process, etc. and also it can be used in very different ways. Checklist puts works in order, so it is used in very different areas. Normally without a checklist, controlling an organisation's standards is hassle. A tool is needed to see whether an organisation comply with specific standards. As a comparison tool in this dissertation project, checklist method is used by author in order to control the organisations whether the organisations compliance with the "**BS ISO 10007:2003**" standards or not? It is aimed to show the organisations' situations in terms of CM, in other words how well they dealt with CM before the accidents happened. Also the checklist helps to distinguish the deficiencies in CM of the organisations.

There are some documents which are very practical to use as guidance for implementing proper CM into organisations. In the UK, two of very common guidance is "**BS ISO 10007:2003**" (ISO, 2003) and "Engineering safety management (the Yellow book)" (RSSB, 2007). According to the document (ISO, 2003), the standards were written to increase the understanding of quality management system and also encourague organizations to apply configuration management. Also aim of CM is to develop companies` performance.

The Yellow book helps organisations about implementation of CM and gives suggestions how CM should implement in organisations. It also gives ideas about the benefits of proper CM to organisations, however the benefits of proper CM is more than it is mentioned in the Yellow book. It was discussed in the literature review section (see chapter 3.1).

4.1 ISO 10007:2003 structure

The document gives guidance about use of configuration management. It is applicable to use it to support a product from planning to disposable. The document cares about responsibilities and authorities, so it outlines them first. Then it describes configuration management process and other topics listed below. The standards document consists of five main chapters apart from foreword and introduction sections. According to the (ISO, 2003), the chapters are respectively presented below.

- Chapter 1which is scope, discusses about function of the document and purpose of the document.
- Chapter 2 which is **normative references**, also recommends use of the document "ISO 9000:2000, **Quality management systems** — Fundamentals and vocabulary" with ISO 10007:2003.
- Chapter 3 which is **terms and definitions** gives definitions of essential terms on the document such as **change control**, **concession** and **configuration**.

- Chapter 4 which is **configuration management responsibility** consists of two subchapters; **responsibilities and authorities,** and **dispositioning authority**. Responsibilities and authorities section describes responsibilities of the organisation which want to implement CM. Dispositioning authority section describes requirements for a change to be approved.
- Chapter 5 which is **configuration management process** consists of six subchapters. They are respectively:
    - **General:** gives idea about configuration management process
    - **Configuration management planning:** gives information about how planning should be, and mentions about importance of planning process.
    - **Configuration identification:** gives general information about product structure and selection of configuration items, product configuration information and configuration baselines.
    - **Change control:** gives general information about change control and discusses following topics, evaluation of change, disposition of change, and implementation and verification of change.
    - **Configuration status accounting:** discusses records, reports and configuration audit.

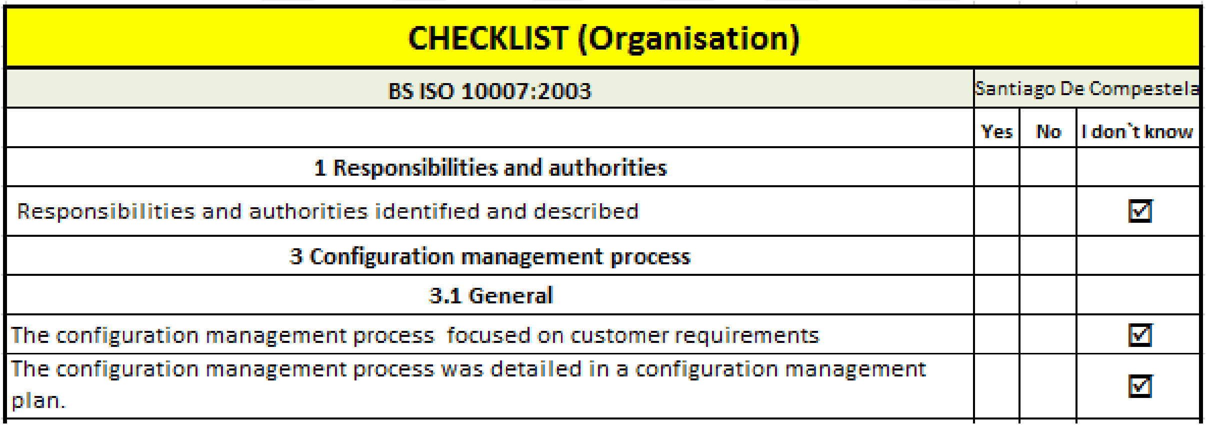
4.2 How the checklist was prepared

In this section, preparation of the checklist is discussed by author. Before passing through the checklist, it is better to know a bit more about the document "**ISO 10007:2003**" The whole name of the document is **Quality Management Systems – Guidelines for Configuration Management**.

4.2.1 Preparation of the checklist

Firstly, the CM standard were read and the sentences which start with should were picked from the standards document. After that, the author chose the appropriate substances for the Santiago accident. These sentences were shortened to take up less space on the checklists. Then these substances were conveyed an MS excel document where a table had drawn on. The table consists of the substances and tick boxes. The tick boxes helps to see which substances were followed by the organisation. Table helps to keep the substances tidy and easily analyse situation of the organisation.

In order to prepare checklist, MS office excel software was used because of its easy use. It consists of five columns which can be seen from the following picture below. For full version of the checklist, see appendix A.



CHECKLIST (Organisation)			
BS ISO 10007:2003	Santiago De Compestela		
	Yes	No	I don`t know
1 Responsibilities and authorities			
Responsibilities and authorities identified and described			☑
3 Configuration management process			
3.1 General			
The configuration management process focused on customer requirements			☑
The configuration management process was detailed in a configuration management plan.			☑

Figure 11 the checklist (Author)

Firstly the checklist was vertically split into two sections. First section includes name of standards and second group includes name of train accidents. Below the name of accident, there are three options and also there is one box below each option. The boxes below options give opportunity to tick. The chapter numbers on the checklist are directly taken from the CM standard document and they refer the numbers on the standard.

The checklist consists of two parts which are Organisational and Change. These parts will be separately introduced on the next chapters.

4.3 How the checklist is used

In this dissertation, the checklist is used to evaluate the accidents, especially Santiago de Compostela train accident. The checklist has four options to choose for each standard. The options are “**yes**”, “**no**”, and “**I do not know**”. According to the author`s opinions, if a requirement is probably complied with, the author ticked the “**yes**” option. If a requirement is not probably complied with, the author ticked the “**no**” option. The author uses secondary data to fill the checklist. Firstly, accidents are worked through and they are written according to their event sequences in following chapters. After explaining the accidents, probable causes are listed and explained with their certain or predicted reasons. By drawing upon on the reasons, the checklist was filled by the author. At the point there is no information about any item on the checklist, those items ticked as “**I do not know**”. The author tries to avoid making predictions about items on the checklist, especially when there are rumours vice versa. Using the checklist shows the deficiencies in CM. The deficiencies in CM are very important to see whether the accidents were preventable with good CM or not?

5 Case Study - Train departed with doors open, Victoria line, LUL

LUL open door incident was chosen because the incident happened after a change and it is thought that better CM could have prevented the incident. On 11 July 2011, a London underground train departed with passengers from Warren street station and all the passenger doors were open at the platform side. After train reached 8 km/h at the same time the train had entered the tunnel and a safety system closed the saloon doors. However the safety system did not close the doors before the train departed. The safety edge door system was fitted to the train in order it to stop the train when it detects a thin object trapped by the doors. The system designed to detect when a shoulder strap or a thin object is caught in the doors. Such a situation may cause an undesired accident if the train departs. The train operator realised that something wrong with the train which had reached 11km/h at that time. Then in order the driver to stop the train, firstly put service brakes on and then emergency brake respectively. Until that time, the train had travelled 14 meters after left Warren street station.

When the train departed from the previous station, Oxford Circus, the safety edge door system was activated. At the Warren street station, the driver omitted to close the doors and also disabled the train door interlock that does not allow the train start before closing the doors. After activation of the safety edge door system at Oxford Circus station, the driver tried to reset the safety edge system but the driver was unable to reset it and at Warren street station, the driver wanted to start the train but the train door interlock does not allow it. Sensitive edge system modification had been implemented, the modification allows the driver to override an activated the safety edge door system which used to be cause service delays on the line. Also the operation of an indication light had been changed most likely misled the driver (RAIB, 2012).

5.1 Sequence of Incidence

The (RAIB, 2012) explains the incident that the train operator departed from Brixton station with train 237 at 17:04 hours. The train reached Oxford circus at 17:17 hours and about 30 seconds later the driver closed the doors. The doors closed visual indicator lighted which represents the doors are closed and the driver pressed the start button. After the driver pressed the start button, the train could not start because the brakes were on. The sensitive edge system had activated and the sensitive edge reset indicator lighted. The TCMS warned the driver and gave a message which shows the location of the door led the system activated. The following picture figure 15 shows the driver cab and locations of the buttons and indicators.

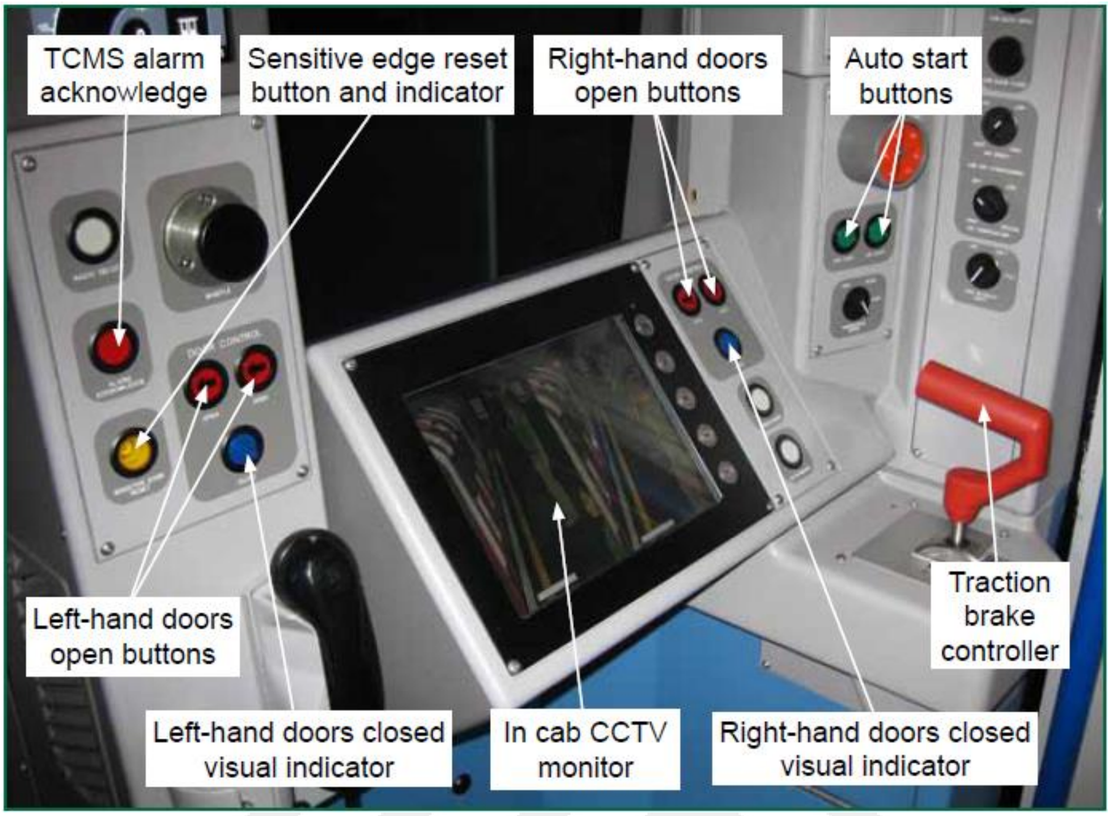

TCMS alarm acknowledge
Sensitive edge reset button and indicator
Right-hand doors open buttons
Auto start buttons
Traction brake controller
Left-hand doors open buttons
Left-hand doors closed visual indicator
In cab CCTV monitor
Right-hand doors closed visual indicator

Figure 12 Layout of relevant cab controls in the driving cab of 2009 tube stock (RAIB, 2012)

In order the driver to reset the sensitive edge system, he pressed the button and then the indicator extinguished. When the sensitive edge system indicator distinguished, the driver thought that the problem was solved and then he attempted to start the train again but the train would not move because the sensitive edge system would not be deactivated and the sensitive edge reset button lighted again.

The driver tried to reset the sensitive edge system but he could not be successful and then he overrode the sensitive edge system. By this way he could start the train and left Oxford Circus station at 17:18 hours. In order to override the sensitive edge system, the driver has to press start button and at the same time he has to keep depressing the reset button until the train left station limits. After 13 seconds the driver realised the sensitive edge reset button and the train automatically stopped because the train had not been outside of the station limits yet.

Then in order to start the train, the driver pressed the sensitive edge reset button a few times and switched the protected manual driving mode, but the attempts were unsuccessful. Also the driver shut down the master control and it broke the round circuit then switched to protected manual. As a result of switching master control down, the door closed relays de-energised and the round train circuit was not completed due to the de-energised relays. In order the driver to isolate the sensitive edge system, he conducted the sensitive edge brake cut out switch, however it did not make a change due to the de-energised door relays. After that the driver turned the sensitive edge brake cut out switch to normal, he tried to take power. Then in the restricted manual mode, he took the power again. The service control called the driver for an update and at that time the driver informed the control centre about his actions. In the meantime, the train waited 5 minutes 46 seconds.

When the train arrived at the Warren street station, it was 17:27:10 hours. When the train reached the Warren Street station, the driver opened the doors at platform side, but the thing caused activation of the sensitive edge system was at the other side of the train. So the thing still remained trapped. The driver attempted to reset the sensitive edge system by pressing the button but he was unsuccessful. Then he restored the round train circuit and he also activated the train door interlock cut out switch.

He again tried to take power but he could not do that. So he again run the round train cut out switch and by this way in protected manual mode he took power again. So he did not close the doors due to he might observe the doors closed visual indicator. It takes about 2 and half minutes the driver to take power. After the train departed from the Warren street, two passengers jumped off from the train onto the platform because the doors were open and then also one passenger tried to run emergency alarm but it was unable to run because the driver had cut the train round circuit. The train doors were closed automatically when the speed had been reached 8 km/h thanks to design of the doors.

Passengers started to shout the driver to stop the train and the driver applied emergency brake by thinking something wrong. When he applied the brake, the speed of the train was 11.07 km/h and the train had travelled 14 metres from the Warren street station. After the train stop, the station supervisor took control and evacuated the passengers. Then the driver drove the train in restricted and protected manual mode to Seven Sister station.

5.2 Probable causes

The probable causes were listed by drawing upon on the report (RAIB, 2012):

1. The driver disabled the train door interlock and then omitted to close the saloon doors. Also in order the driver to realise the brakes, he cut out the train round circuit when the sensitive edge system was activated.
2. The driver did not take the train out of service when he struggle dealing with the sensitive edge system. According to the LUL`s instructions, he should have taken the train out of service.
3. The train driver was determined to keep the train in service. He tried to keep the train in service until the destination Seven Sisters and he thought that he could take the train out of service there.
4. During his action, the driver was observing by the Victoria line service control and the service control was aware of the driver had performed isolations but the control service did not instruct the driver. The control service believed that at Euston station which is next station after Warren Street, the doors where the bag trapped were going to be open and the driver was going to be able to reset the sensitive edge system.
5. By using cut out switch the driver disabled the train door interlock to start the train at Warren Street station.
6. A bag trapped by the doors and as usual the sensitive edge system was activated but the way the driver used to reset the sensitive edge system was a factor of the incident.
7. The sensitive edge system override modification made the driver confused besides the sensitive edge reset light extinguished when the system was still activated. Also the TCMS display message used to be `Emergency brake applied, once cause of activation is **resolved** press sensitive edge push button for brake realise`. And in May 2011, the TCMS display message was changed to ` Emergency brake applied, once cause of activation is **known** press sensitive edge push button for brake realise`. So this modification led the driver to think that he knows the cause of the activation and pressed the sensitive edge reset button without solving the problem.
8. Activation of the sensitive edge system and efforts of the driver to reset the system made him confused.

5.2.1 The Change

The change on the following checklist is Sensitive edge override modification which allows train operators to override sensitive edge system when the system is activated. The modification was implemented due to service delays when the passenger’s belongings are trapped by the train doors.

5.3 Basic Application of the Accident Causation Models

5.3.1 Reason's model

According to the model reacted by Reason (1997):

The hazard: Travelling of the train with doors open.

The defences: Training of driver and the train door interlock

Unsafe acts: Deactivation of the train door interlock and not taking train to out of service

Local factors: Pressure to keep train in service and time pressure

Organisational factors: Modification of the sensitive edge system override (see the chapter 5.2.1) and lack of training about the system.

It can be seen that the Reason's model helps to comprehend the incident and define causation of the incident. As Reason (1997) says that unsafe acts make holes on the defences and only few of them can breach the defences and result with losses. In this incident, the driver was confused and it misleads the driver. Respectively, the driver deactivated one of the defences and it resulted with incident.

5.3.2 Leveson's model

According to the Leveson (2011)'s model, the constraints should be enforced to prevent incident. There are two main points which caused the incident. The points:

- Modification of the sensitive edge override
- The driver did not take the train out of service when he first faced the problem

Before modification, LUL should have been done necessary risk assessments and at least in order the LUL to prevent the drivers from confusion, they should have trained the drivers about the system.

The constraint about the train is to prevent the train from departure when the doors open. The constraints about the driver are to know how to deal with the system and to take the train out of service when he first met the problem and it is written on LUL's instructions. Although the instruction enforces the driver to take train out of service, he made an effort to keep the train in service and it might be due to environmental factors like time pressure. The driver should have been given trainings about actions he needs to take in case of such a scenario. The constraint about LUL is to train the drivers about the system.

5.4 Checking configuration management standards by using the checklist

At first the author applied **the organisational checklist** to LUL and standards were controlled with LUL. No deficiencies were discovered at the organisational side of CM, so the organisational checklist was not presented here.

Table 1 the configuration management checklist for the change (Author)

CHECKLIST (Change)			
BS ISO 10007:2003	**LUL**		
	Yes	**No**	**I don`t know**
2 Dispositioning authority			
Verified that the proposed change is necessary	□	☑	□
The change was documented and categorized	□	□	☑
The planned activities were satisfactory.	☑	□	□
4 Change control			
4.1 General			
After the initial release of product configuration information, all changes were controlled.	□	□	☑
The process for controlling the change was documented, and should include the following:	□	□	☑
• A description of, justification for, and record of, the change;			
• A categorization of the change, in terms of complexity, resources and scheduling;			
• An evaluation of the consequences of the change;			
• Details of how the change should be dispositioned;			
• Details of how the change were implemented and verified.			
4.2 Initiation, identification and documentation of the need for change			
Change proposals typically included the following information:	□	☑	□
• A description of the proposed change;	□	☑	□
• Details of other configuration items or information that may be affected by the change;			
• The interested party preparing the proposal, and the date it was prepared;			
• The reason for the change;			
• The category of the change.			
The status of change processing, the related decisions and the dispositions were documented.	□	□	☑
4.3 Evaluation of change			
4.3.1 Evaluations concerning the proposed change was performed and documented.	□	☑	□
The technical merits of the proposed change	□	□	☑
The risks associated with the change	□	☑	□
The potential impact on contract, schedule and costs	□	□	☑
4.4 Disposition of change			
A process was established for the disposition of change that identifies the dispositioning authority (see 4.2) for each proposed change.	□	□	☑
The disposition was recorded.	□	□	☑
4.5 Implementation and verification of change			
After implementation, compliance with the approved change was verified. This verification was recorded to allow traceability.	□	☑	□

Preparation of the checklist is explained in the chapter 4, so it will not be explained here again. The organisational and the change checklists are illustrated on the table 2 and 3 above. The checklist helps to find deficiencies in CM (see the chapter 4.3 for filling of the checklists). According to the checklist, the deficiencies are identified. Those deficiencies shows CM situation in the organisation. The author also discuss about whether those deficiencies could be dealt with by the organisation before the train crash.

5.5 Deficiencies in configuration management

- Deficiencies from the change checklist (RAIB, 2012):
  - "Should verify that the proposed change is necessary, and the consequences would be acceptable" this requirement requires that the change is necessary. The change which mentioned above and in the light of the report (RAIB, 2012) the change seems that TCMS display message change is not necessary and also it misled the driver and it is also 7th causes of the incident (see the chapter 5.2). The display message used to advise drivers to push the button if they resolve the cause of activation but after modification the display message advices drivers to push button if they know the cause of activation. So it does not require resolving the cause of activation and does mislead the drivers.
  - There was not any description of the functional of the proposed change, so it also negatively affected the train operator.
  - Evaluation of the change should be performed and documented, although the report shows that a risk assessment of the technical aspect of the change was carried out by Bombardier, but the risk assessment does not cover operational aspect of the modification. However LUL did not carry out a risk assessment of the operational aspect of the modification.

6 Case Study - Santiago de Compostela train accident

The date 24th of July 2013 is a worse train crash in Spain because after 40 years later from the train crash in Seville (Infoplease, 2014), the country again witnessed a bitter train derailment in Santiago de Compostela. The Alvia 730 series train, which is being operated by Renfe stated owned company, derailed on a curve which is 4 km outside of the Santiago de Compostela station when it was travelling from Madrid to Ferrol in Spain (BBC, 2013). The high speed Alvia train with 218 passengers and 4 crews entered the curve at speed 190 km/h just before the train was come off the tracks and derailed on the curve at 20:40 local time. As a result of the accident, 79 people died and around 140 people injured. The speed limit is 80 km/h for the curve where the derailment occurred. Most part of the route equipped ERTMS (European Rail Traffic Management System) but the curve had only Spain train protection system which is ASFA (“Automatic Braking and Announcement of Signals” in English) (Railway Gazette, 2013). The train protection systems such as ERTMS and ASFA protect trains from over speeding and warn drivers via audio or screen on drivers cab when they exceed the speed limit.

6.1 The accident sequence

The black box reports (Sky News, 2013) says that the Alvia 730 series hybrid train made departure from Madrid Chamartin station to Ferrol station at 15:00 on 24th of July 2013. When it was about 20:39 hours, the train was travelling at speed 195 km/h near the last tunnel before the curve where the accident happened on.

Also at that time the driver was warned by train protection system (ASFA) to slow down the train, but he did not slow. In the time 20:40 he got another warning again, he did not slow the train down. The speed limit was 80 km/h while he was travelling at speed of 195 km/h on the line. There was 11 seconds for derailment of the train when the driver just finished his call to the on-board conductor. The conductor phoned the driver in order to discuss about the later platform. When there were 250 m to the curve, the last warning came. The driver noticed the last warning and tried to slow down the and right after applied emergency brakes when four seconds after the last warning. Although the driver applied emergency brakes, it was too late slow down train from 195 km/h to 80 km/h within such a very short distance.

The last action of the driver helped to slow down train to speed of 179 km/h which was still more than double speed limit on the curve. When it was 20:41 hours and due to high speed on the curve, first middle coaches of the train lost wheel-rail contact and then the locomotive lost the contact. The report pointed that "At 20:41:06 the sound of the dragging of the train produced by the derailment is heard. At 20:41:16 the sound of dragging ends." The thirteen coaches of train derailed and crashed the concrete wall by the track. One of the coaches flung from the track to on the embankment wall by the track as soon as the train derailed.

The people around the accident scene heard the voice of crash and right after they called the emergency service to report the accident. The result of the accident, 79 passengers were killed and around 140 people on- board were injured. The driver survived as injured and he is the key to discover main reason of the accident.

6.2 Possible scenarios

In this section, it is tried to discover that what the main causes of the Santiago accident are. The following scenarios were founded from the websites; it means the information is secondary data. The accident report of the accident has not been published, so following scenarios are predictions.

6.2.1 The driver did not slow down

Train drivers are educated about the train and the route which they will use. The training session for drivers may take months before driving real train and route. Also train drivers know the routes very well otherwise they do not have permission to drive on those routes. Normally train drivers follow instructions from on-board screen and according to the instructions they make action. Train drivers comply with speed limits on routes otherwise it may ends with an accident like happened in Santiago de Compostela. As mentioned above that the driver was warned three times by train protection systems in two minutes before the derailment. Even though he applied emergency brakes after four seconds from the last warning, he was not able reduce the train speed at appropriate level.

In normal situation drivers know the routes and they know where to slow down, so the driver might have felt confident about the route and applied brakes late. According to the (Sky News, 2013), the driver said after the crash that "I tell you sincerely that I don't know. Otherwise I would not have been so crazy as not to brake" and also he told the judge "I can't explain. I still don't understand," It can be understood from the driver`s action that one of the main causes was him. The driver should take care of passengers` life and health on-board.

6.2.2 Automatic train protection system deficiency

Ourense and Santiago route is equipped with ETCS level 1 and ASFA signalling which are train protection systems. However the curve was only equipped with ASFA. According to (Puente, 2013), the ETCS on-board equipment switched off, so the ETCS was not working on the high speed line when accident happened. It shows that they put all the responsibilities on the driver’s shoulders, because ASFA only stops the train if it goes at speed more than 200 km/h.

The Renfe should have taken some precautions to prevent the accident for example; before switching off the ETCS, preparing a proper risk management plan. Normally if driver goes over speed limit, train protection system warns the driver and waits for a certain time to be acknowledged by the driver. If the driver does not acknowledge the system within the certain time, the train was stopped by automatic train protection system (see chapter 2.5). In the light of such information, one of the main causes is that ASFA signalling system on the line does only stop the trains if the speed is over 200 km/h. Otherwise it just warns drivers about the speed limit on the line.

6.2.3 Lack of signage for speed limit

The figure 16 below shows that there is not any speed limit signage at the last tunnel entry or there may be a signage but not clear.

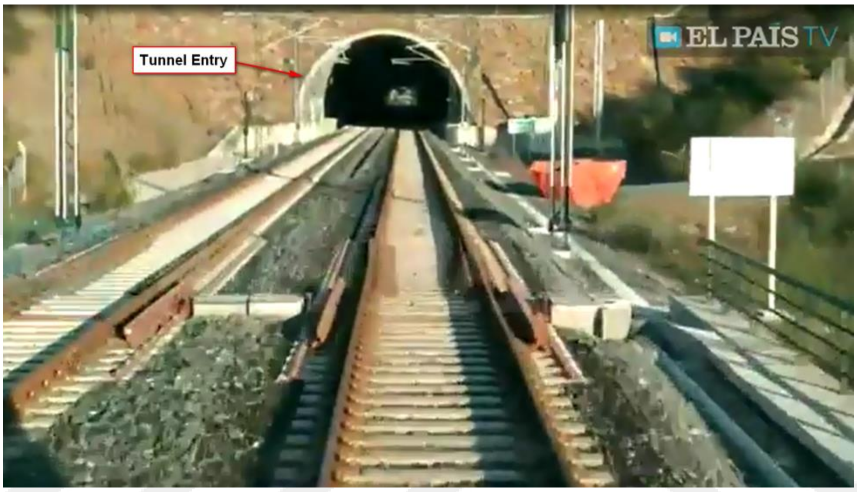


Figure 13 the last tunnel before the curve (www.elpais.com)

There is a board at right hand side on the figure 16 but it is not readable due to sunlight. This is not a main reason of the crash because the driver was even warned by train protection system (see the chapter 6.1). Therefore signage is not a main problem with the lines equipped with ATP systems.

6.2.4 Sabotage

On the some website, the first thing coming to mind was sabotage, but there is no evidence that was a sabotage attack to railway. Therefore there is no necessary to explain sabotage possibility here.

6.2.5 The change

As mentioned before Renfe wanted the drivers to switch off ETCS on-board without doing proper risk assessment. The change represents the switching off the ETCS on driver's cab. Therefore it always was mentioned as the change on the checklist and sometimes on following chapter as well.

6.3 Basic Application of the Accident Causation Models

6.3.1 Reason's model

According to the Reason's model:

Hazard: Driving a high speed train

Defences: Signalling systems, automatic train protection system, and training driver

Unsafe acts: Not considering warnings,

Local factors: Number of tunnels on the line, calling conductor

Organisational factor: Switching off ETCS, insufficiency of ASFA signalling, rapid speed reduction

There were some holes on the defences such as the ASFA stops the train only when the train goes over than 200 km/h, however the speed limit was 80 km/h on the curve. Another defence was ETCS which used to warn driver at the transition point where very close the curve, so the drivers used to know they were approaching the dangerous curve. Besides these holes on the defences, the driver made vital unsafe act which he ignored the warnings and applied the brake late.

He said that he did not know his location just before the derailment. It was due to local factors such as there are 31 tunnels on the line between Ourense and Santiago. So it misled the driver to confuse. He was on phone to on-board conductor, so it might affect the driver to ignore or not hearing the warnings. So the organisational factors, the local factors and unsafe acts of driver contributed the accident.

6.3.2 Leveson's model

According to the Leveson's model, the constraints should have prevented the train from going faster than the speed limit as a result of accidents. The main reasons of the derailment are: lack of train protection system and the driver ignored the warnings.

The constraint about the train protection system is to stop the train when it exceeds the speed limit. The constraint about the driver is to acknowledge the train protection system and not going faster than speed limit. The constraints about the organisation are to train the drivers and control protection systems and to observe risks of driving high speed train on the line.

The Renfe should have not switched off ETCS and also should have considered the curve as a danger before the accident happened. After accident, the Renfe installed new balises to restrict drivers not going faster than speed limit. But it is a late action and it should have been taken earlier.

6.4 Checking configuration management standards by using the checklist

Table 2 the configuration management checklist for the organisation (Author)

CHECKLIST (Organisation)			
BS ISO 10007:2003	Santiago De Compostela		
	Yes	**No**	**I don`t know**
1 Responsibilities and authorities			
Identified and described responsibilities and authorities	□	□	☑
3 Configuration management process			
3.1 General			
The configuration management process focused on customer requirements	□	□	☑
The configuration management process was detailed in a configuration management plan.	□	□	☑
3.2 Configuration management planning			
The configuration management plan for a specific product • Documented and approved	□	□	☑
• Controlled	□	□	☑
• Identified the configuration management procedures to be used	□	□	☑
• Made reference to relevant procedures of the organization wherever possible	□	□	☑
• Described the responsibilities and authorities	□	□	☑
3.3 Configuration identification			
3.3.1 Product structure and selection of configuration items			
The selection of configuration items and their inter-relationships described the product structure.	□	□	☑
Configuration items were identified using established selection criteria.	□	□	☑
Configuration items were selected to achieve the overall end-use performance of the item.	□	□	☑
The number of configuration items selected optimizes the ability to control the product.	□	□	☑
The selection of configuration items was initiated.	□	□	☑
The configuration items were reviewed as the product evolves.	□	☑	□
3.3.3 Configuration baselines			
Configuration baselines were established.	□	□	☑
5 Configuration status accounting			
5.1 General			
The organization performed configuration status accounting activities throughout the life cycle of the product.	□	□	☑
5.2.2 The evolving product configuration information was recorded in a manner that identifies the cross-references and interrelationships necessary to provide the required reports (see 5.5.3).	□	□	☑
6 Configuration audit			
Configuration audits were performed in accordance with documented procedures.	□	□	☑

Table 3 the configuration management checklist for the change (Author)

CHECKLIST (Change)			
BS ISO 10007:2003	Santiago De Compostela		
	Yes	**No**	**I don`t know**
2 Dispositioning authority			
Verified that the proposed change is necessary	□	☑	□
The change was documented and categorized	□	□	☑
The planned activities were satisfactory.	□	☑	□
4 Change control			
4.1 General			
After the initial release of product configuration information, all changes were controlled.	□	□	☑
The process for controlling the change was documented, and should include the following:	□	□	☑
• A description of, justification for, and record of, the change;			
• A categorization of the change, in terms of complexity, resources and scheduling;			
• An evaluation of the consequences of the change;			
• Details of how the change should be dispositioned;			
• Details of how the change were implemented and verified.			
4.2 Initiation, identification and documentation of the need for change			
Change proposals typically included the following information:	□	□	☑
• A description of the proposed change;			
• Details of other configuration items or information that may be affected by the change;			
• The interested party preparing the proposal, and the date it was prepared;			
• The reason for the change;			
• The category of the change.			
The status of change processing, the related decisions and the dispositions were documented.	□	□	☑
4.3 Evaluation of change			
4.3.1 Evaluations concerning the proposed change was performed and documented.	□	☑	□
The technical merits of the proposed change			
The risks associated with the change			
The potential impact on contract, schedule and costs			
4.4 Disposition of change			
A process was established for the disposition of change that identifies the dispositioning authority (see 4.2) for each proposed change.	□	□	☑
The disposition was recorded.	□	□	☑
4.5 Implementation and verification of change			
After implementation, compliance with the approved change was verified. This verification was recorded to allow traceability.	□	☑	□

6.4.1 Deficiencies in configuration management

The deficiencies are respectively listed from the organisational checklist to the change checklist. The quotations below were taken from the document (ISO, 2003).

- CM deficiencies from the organisational checklist
  - "The configuration items should be reviewed as the product evolves." According to this requirement when the new line between Santiago de Compostela and Ourense was opened, the configuration items which are ASFA and ERTMS signalling system should have been reviewed. However the evidences show that the signalling system ERTMS was switched off and also there was not communication between ASFA and ERTMS signalling (see the chapter 6.2.2). So not fully complied with when ERTMS was switched off.
- Deficiencies from the change checklist.
  - "Should verify that the proposed change is necessary, and the consequences would be acceptable." As mentioned above that switching off the ERTMS signalling on drivers cab needs to be reviewed before implementation of it because it leaves the train unsafe and safety is just loaded on driver's shoulders. ASFA signalling intervenes when the train goes above 200 km/h, but speed limit was only 80 km/h. So ASFA signalling was not able to anything apart from warning the driver about speed limit.
  - "The planned activities for the implementation of the change into documents, hardware and/or software are satisfactory." The Renfe asked the drivers to implement the change, but the Renfe did not plan the change and just want to solve delay problems by switching off ETCS.
  - "5.4.3.1 Evaluations concerning the proposed change should be performed and documented. The extent of any evaluation should be based on the complexity of the product, the category of the change." The accident shows that the change was not properly evaluated and proper risk assessment was not made by the organisation.
  - "After implementation, compliance with the approved change should be verified. This verification should be recorded to allow traceability." The problem with this requirement is that the change was not approved and verified before the accident.

The deficiencies are immobilised by using the checklists. To make deficiencies clear, there are some omissions such as switching off the ERTMS on drivers cab without doing risk assessment. The checklists showed that the organisation did not do proper CM and the deficiencies are the proofs of it. The questions; why was not the whole line equipped with ERTMS level 1? And why does ASFA signalling only stop the trains which go faster than

200 km/h? These questions led the author to concentrate on CM deficiencies on the organisation. As mentioned above that there are two types of signalling system on the route and the signalling systems used to switch to another just 4 km before the curve where the accidents happened. Also the ASFA signalling system was not totally safe because it just warned the driver and did not stop the train before the accident. Normally automatic train protection system warns drivers if they go faster than speed limit and even train protection systems stops train when drivers do not responded the warnings (Connor, et al., 2014). The railway should not just relay on drivers in terms of safety, because mankind have potential to do mistakes.

The mistakes or omissions, emphasis on the importance of configuration management in safety critical systems like railways. The chapter 7 gives the answer of the question, “Could proper configuration management prevent the accident?”

7 Could proper CM have prevent these accidents?

7.1 Train departed with doors open, Victoria line, LUL

As mentioned at the chapter 5, the driver was not able deal with the sensitive edge system on the train and the system had been installed in 2009. When the sensitive edge system was activated at Oxford circuit station, the driver tried to reset the system by pressing the sensitive edge system reset button. The sensitive edge activation light turned off when the system was activated, so the driver thought the cause of activation was solved. But he could not reset the system and he overrode the sensitive edge system instead of checking the platforms, inside the train and opening and closing doors until he resolve the cause of activation. The TCMS display message had misled the driver because the message was changed in May 2011 (RAIB, 2012).

Therefore the driver did not want to lose time and he thought that he knows the cause of activation, so he pressed the button to realise brakes. He could not start the train and then he overrode the sensitive edge system without solving the cause.

7.1.1 The results of proper configuration management in the organisation

One of the main requirements of the configuration management standards is that evaluation of the risks associated with the change should be performed and documented (ISO, 2003). The RAIB report shows that LUL did not carry out a risk assessment of operational aspect of the change although the bombardier carried out a risk assessment of technical aspect of the change. So risks of implementation of the change were not identified from operational side of the change (RAIB, 2012).

Although the change modification of sensitive edge override was not only cause led to the incident, it was one of the main causes of the incident. If proper configuration management was done in LUL, the organisation would take some precautions to prevent drivers from confusion. So, proper configuration management would have prevented the organisational factors discovered by using Reason’s model (see the chapter 5.3.1) and also would have enforced the constraints from Leveson’s model (see the chapter 5.3.2). The organisational factors and the constraints are main factors of the incident, so prevention of them means prevention of the incident.

During this incident, no one was hurt but someone could hurt themselves for instance; someone could fall down on the rails after the train departed from the Warren Street station. So it would have led to a more terrible situation.

The deficiencies in the change checklist are;

- The change should be verified,
- A description of the change should be provided

- Risk assessment of the change,
- The change should be controlled after implementation of it (ISO, 2003).

It can be said that these requirements enforce LUL to carry out a risk assessment before implementation of the change and it is expected that if the risk assessment of operational aspect of the change carried out by LUL, misleading of the TCMS display message would be predicted and by drawing upon on the risk assessment, LUL would seek solutions for the confusion. LUL did not know what the change was exactly, so the driver could not deal with the override modification. If LUL had description of the proposed change, LUL would have trained the train operators about the sensitive edge system override modification. Therefore, if proper CM had been done, the incident would have been prevented.

7.2 The Santiago de Compostela train accident

The Santiago train derailment happened due to inadequacy of the train protection system and the driver’s mistake, so was not it preventable? The accident seems to be happened due to the driver’s mistake. It is because they put all the responsibilities on the driver shoulders, in other words the safety of the train was on the hands of driver. Therefore first impression and general impression on the driver’s mistake going too fast on the curve. However there must be some systems which provide safety drive on the route. Like many modern railways, the Santiago line had got train protection system but two different types (HOOPER, 2013). However both of those train protection systems could not prevent the train from derailment, because one of them (ERTMS) was switch off and the other was not able to stop the train at that speed. The accident shows that proper configuration management might prevent the accident.

The main deficiencies in terms of configuration management:

- Switching off the ERTMS signalling on the driver’s cab might be verified by Renfe that it was a necessary action but the results of the action should have been reviewed. The necessary risk assessment should have been done before implementation.
- Implementation of the change should have been satisfactory, but it was not. The planned activity for implementation of the change might be necessary, but result of the implementation was not satisfactory.
- Evaluation of the change should have been documented, but either the organisation might misevaluated the change or they did not evaluate the change. Because if they correctly evaluated the change, they would have predicted the accident as a result of the change.

These are the issues which are related to configuration management in the organisation. In this point, the author looks at the result if the organisation did proper configuration management before the accident.

7.2.1 If better configuration management had been done

The substances below are prediction of the author and they present the situation as if the organisation did proper configuration management.

- The organisation would review the signalling and train protection systems when they built the Santiago – Ourense line. They might have chosen to use ERTMS for the whole line or the curve would have equipped with more balises which can stop train at the speeds 30 km/h, 60 km/h and 160 km/h. After the derailment, the members of the development committee were informed that new ASFA balises will be installed at locations where there is big reduction in speed limit (RIG, 2013). After that the organisation equipped the line with this kind of balises but after the derailment (ERTMSnews, 2013). This precaution should have been taken in the beginning.
- The organisation would verify the change to switch off the ERTMS signalling would have found that the consequences of the change of the change are not acceptable and would have put in place more precautions.
- Even if the change was not a planned activity, the organisation would have controlled all the changes according to the configuration management standards.
- The risks associated with the change, would be considered before the accident.

On the one hand, besides the above, proper configuration management would have prevented the organisational factors and would have enforced the constraints (see the chapter 6.3). These are the main causes of the accident.

On the other hand, the checklists showed that thanks to proper configuration management, the organisation would have done risk assessments and taken precautions about train protection system. As mentioned before that Renfe wanted the drivers to switch off ETCS driver’s cab signalling (see the chapter 6.2.5). However, at the transition point the driver had to acknowledge ETCS that he knows that the signalling systems are switching. Also the transition point used to help the drivers to remember the tight curve. On the line Santiago-Ourense, there are 31 tunnels and the curve comes just after a tunnel, so it is not easy to remember the tight curve. However, it used to be easy for the drivers to remember the curve thanks to the transition point. After implementation of the change the drivers had to remember which tunnel comes before the curve, so it means the drivers had to more careful than before. Also the ASFA balises just stops the trains if the speed is above 200 km/h while the speed limit is 80 km/h on the curve. According to (ISO, 2003) “should be verify that the proposed change is necessary, and the consequences would be acceptable”. However the result of Santiago train derailment is not acceptable because 79 people were killed on the crash. Proper configuration management would have helped to see the risks of the change and to put in place precautions which would have prevented the accident. So if proper CM had been done, the Santiago accident would have been prevented.

8 Conclusions

8.1 Findings

In this project, the author worked on two cases which are the Santiago train accident and the LUL open door incident. Both of the cases were reviewed to see could proper CM have prevented these accidents.

In order to understand how CM should be done, the yellow book provide sufficient guidance and the yellow book reviewed with its deficiencies in the literature review chapter. In addition, popular and at some point similar two models; Reason`s (Swiss cheese) and Leveson’s (STAMP) accident causation models were reviewed their criticisms. These models help to better understand how accidents happen.

In this project the main causes of the accident and incident were listed and also the deficiencies in configuration management were founded by using the checklists. The deficiencies were discovered that they are related to some of the main causes of the accidents. If better configuration management had been done, the accidents would have been prevented. A table below was generated to show relations between the main causes and CM deficiencies.

Table 4 Relation between the causes and the deficiencies (The author)

The related causes of accident/incident	The related deficiencies in CM
LUL open door incident	
The TCMS display message change	Verified that the proposed change is necessary and results are acceptable.
	Evaluation of the change should be performed and documented
Santiago train accident	
Switching off ETCS	Verified that the proposed change is necessary and results are acceptable.
	Evaluation of the change should be performed and documented
	Evaluations concerning the proposed change should be performed and documented
	After implementation, compliance with the approved change should be verified

This project shows that the changes had important contribution on the accidents. If the changes were made by complying with CM standards, these accidents would have been predicted and to put in place precautions which would have prevented the accidents.

In order to see how accidents happened two accident causation models; Reason's and Leveson's models were used. They are good tools to find causations, but although the Reason's model simple and easy to use, it is unsufficient to see root causes of accidents. The Leveson's model helps to see root of the causes and to put in place precautions for future losses. But it needs to put more effort to analyse accidents. These two models also helped to find main causes of the incident and accident.

In the Santiago accident, 79 passengers were killed and it cannot be changed. However some future accidents could be prevented thanks to proper CM. This project helped to see important of the CM in these accident and incident that CM requires to do risk assessment before a change and to be sure that the results of the change is acceptable. Therefore the author thinks that CM is not just keeping tracks of related things and their relationships, it is also a fuse which prevent systems from dangerous change for the organisations.

Organisations cannot easily foresee the potential accidents before accidents happen. They usually think that their organisations do not have risks, so they do not take precautions to prevent accidents. If organisations can foresee potential accidents, they would put precautions to provide safety. Proper CM helps to see risks on organisations and prevent organisations from bad decisions. Accidents harm organisations in terms of losses, bad impression, and damage cost. It means if potential accidents are prevented, organisations will not lose money and their popularity above all they may save lives. Although organisations need to have extra budged for CM, they will save more money and lives thanks to CM. So, the money invested on safety is not dead investment.

8.2 Recommendations

- CM may prevent some future vital accidents, so it is strongly recommend that especially in safety critical systems, CM should be done if the organisations can afford to do it.
- If the world does not want to see accidents like the Santiago accident one more time, the railway organisations and safety critical organisations should consider CM option.
- CM may be expensive for some organisations due to its requirements, so organisations should start doing CM if they are going to do proper CM. Otherwise it unsufficient CM might not help to prevent accident and it might just be extra work for the organisation.
- Training is very crucial in organisations to prevent losses, so besides the proper CM, people in the organisations should be trained well about the safety.
- People, who are responsible for following CM in the organisations, should be well trained and should be aware of importance of proper CM.
- Organisations should review their safety before they face losses and take precautions.

- In order organisations to prove they keep risks at lower level, CM is a good way to show it to other people.

8.3 Review of Approach

In this project, in order to investigate configuration management in those organisation, the author chose to prepare checklist by drawing upon on the (ISO, 2003) document. The checklist helps to compare the CM standards and the organisations and to see whether the organisations did proper CM. Thanks to the checklists, the deficiencies in CM were easily detected and presented. The ISO CM standards were selected because thanks to the list of requirements on the standard, CM can easily be implemented in organisation.

In addition, in order to find the cause of the accident and incident, the accident causation models were simply applied to the case studies. Both models were reviewed in the literature review chapter.

8.4 Areas for Further Work / Research

This project covers effects of proper CM on the case studies; a further work can be done on:

- What kind of organisations should do proper CM?
- What are the results of proper CM in organisation which did proper CM?
- What is the cost of proper CM for a certain railway organisation?
- Why organisations should do proper CM?
- How CM can be popularized within organisations?

8.5 Word Count

There are 14610 words between sections 1 and 8.4.

9 References

9.1 Documents

Abed, S. K., 2010. *European Rail Traffic Management System – An overview,* s.l.: Iraq J. Electrical and Electronic Engineering.

Dekker, S., 2002. *The Field Guide to Human Error Investigations,* s.l.: Ashgate Publishing Limited .

EIA, 2004. *National Censensus Standard for Configuration Management,* Arlington: Electronics and Information Technology Association.

Elliott, M., Page, K. & Worral-Carter, L., 2012. *Reason`s Accident Causation Model: Application to adverse event in acute care,* Sippy Downs: eContent Management Pty Ltd.

Hidden, A., 1989. *Investigation into the Clapham Junction Railway Accident,* London: Department of Transport.

ISO, 2003. *ISO 10007:2003 Quality management systems -- Guidelines for configuration management,* London: International Organization for Standardization.

Leveson, N., Daouk, M., Dulac, N. & Marais, K., 2003. *Applying STAMP in Accident Analysis,* Cambridge: Investigation and Reporting of Incidents and Accidents (IRIA).

Leveson, N. G., 2011. STAMP: An Accident Model Based on System Theory. In: J. Moses, ed. *Engineering a safer world.* Cambridge: the MIT press, pp. 73-100.

Luxhøj, J. . T. & Kauffeld, K., 2003. *Evaluating the Effect of Technology Insertion into the National Airspace System,* New Jersey : The Rutgers Scholar.

Müller, P., 2013. *Configuration Management - a core competence for successful through-life systems engineering services,* Bremen: Elsevier.

Qureshi, Z. H., 2008. *A Review of Accident Modelling Approaches for Complex Critical Sociotechnical Systems,* Edinburgh: Defence Science and Technology Organisation (DSTO).

RAIB, 2012. *Train departed with doors open, Warren Street, Victoria Line, London Underground, 11 July 2011,* London: Department for Transport.

Reason, J., 1997. *Managing the Risks of Organizational Accidents.* 1st ed. Aldershot: Ashgate Publishing Limited.

RIG, 2013. Safety principles under review. *Railway Gazette International,* Issue 009/13, p. 25.

RSSB, 2007. *Engineering Safety Management (Yellow book).* London: Rail Safety and Standards Board.

RSSB, 2010. *ETCS System Description,* London: RSSB.

Shappell, S. A. & Wiegmann, D. A., 2000. *The Human Factors Analysis and Classification System - HFACS,* Virginia: US Department of Transportation.

Song, Y., 2012. *APPLYING SYSTEM-THEORETIC ACCIDENT MODEL AND,* Ontario: McMaster University.

Transport for NSW, 2011. *A brief introduction to the Railcrop Automatic Train Protection (ATP) system,* Chippendale: Transport for NSW.

University of Aberdeen, 2003. *Factoring the human into safety: Translating research into practice,* Aberdeen: Health and Safety Executive.

9.2 Web Site Links

Adif, 2012. *Madrid-Galicia line.* [Online]
Available at: http://www.adif.es/en_US/infraestructuras/lineas_de_alta_velocidad/madrid_galicia/madrid_galicia.shtml
[Accessed 04 June 2014].

Adif, 2012. *Ourense-Santiago Corridor.* [Online]
Available at: http://www.adif.es/en_US/infraestructuras/lineas_de_alta_velocidad/madrid_galicia/ourense_santiago/ourense_santiago.shtml
[Accessed 06 June 2014].

ELPAIS, 2013. *ADIF and Renfe review their safety protocols after the accident.* [Online]
Available at: http://ccaa.elpais.com/ccaa/2013/07/29/galicia/1375128308_818675.html
[Accessed 09 07 2014].

ERTMSnews, 2013. *ADIF already puts new ASFA balises in ERTMS transition areas.* [Online]
Available at: http://www.ertmsnews.com/2013/08/03/adif-already-puts-new-asfa-balises-in-ertms-transition-areas/
[Accessed 12 07 2014].

ERTMSnews, 2013. *RENFE asked to switch off ERTMS nearly nine months before the Santiago accident.* [Online]
Available at: http://www.ertmsnews.com/2013/08/03/renfe-asked-to-switch-off-ertms-nearly-nine-months-before-the-santiago-accident/
[Accessed 09 07 2014].

ERTMSnews, 2013. *Santiago de Compostela accident: no ERTMS installed at site.* [Online] Available at: http://www.ertmsnews.com/2013/07/26/santiago-de-compostela-accident-no-ertms-installed-at-site/
[Accessed 09 07 2014].

HOOPER, J., 2013. *Spanish train crash: automatic braking on notorious curve failed to engage.* [Online]
Available at: http://www.theguardian.com/world/2013/jul/25/santiago-train-derailment-speed-safety
[Accessed 30 06 2014].

Infoplease, 2014. *Railroad Accidents.* [Online]
Available at: http://www.infoplease.com/ipa/A0001450.html

Puente, F., 2013. *Adif president to give evidence in Santiago inquiry.* [Online] Available at: http://www.railjournal.com/index.php/europe/adif-president-to-give-evidence-in-santiago-inquiry.html

Railway Gazette, 2013. *Overspeed suspected in Santiago de Compostela derailment.* [Online] Available at: http://www.railwaygazette.com/news/single-view/view/overspeed-suspected-in-santiago-de-compostela-derailment.html

Railway Gazette, 2013. *RENFE restructuring approved.* [Online]
Available at: http://www.railwaygazette.com/news/policy/single-view/view/renfe-restructuring-approved.html
[Accessed 03 June 2014].

Sky News, 2013. *Spain Train Crash: Black Box Data Disclosed.* [Online]
Available at: http://news.sky.com/story/1123842/spain-train-crash-black-box-data-disclosed

Spain Ministry of Development, 2014. *Structure of railway sector in Spain.* [Online]
Available at:
http://www.fomento.es/MFOM/LANG_CASTELLANO/DIRECCIONES_GENERALES/FERROCARRILES/Estructura_ferr/
[Accessed 06 June 2014].

Talgo, 2013. *Rolling Stocks.* [Online]
Available at: http://www.talgo.com/index.php/en/material.php
[Accessed 10 08 2014].

10 Appendix

10.1 Appendix A

CHECKLIST (Organisation)				
BS ISO 10007:2003	Santiago De Compostela			
	YES	**NO**	**N/A**	**I don`t know**
4.1 Responsibilities and authorities				
The organization identified and described responsibilities and authorities related to the implementation and verification of the configuration management process.				
5 Configuration management process				
5.1 General				
The configuration management process should focus on customer requirements for the product and should take into account the context in which it will be performed.				
The configuration management process should be detailed in a configuration management plan. This should describe any project-specific procedures and the extent of their application during the life cycle of the product.				
5.2 Configuration management planning				
The configuration management plan for a specific product should be documented and approved				
• should be controlled				
• should identify the configuration management procedures to be used				
• should make reference to relevant procedures of the organization wherever possible				
• should describe the responsibilities and authorities for carrying out configuration management throughout the life cycle of the product.				
5.3 Configuration identification				
5.3.1 Product structure and selection of configuration items				
The selection of configuration items and their inter-relationships should describe the product structure.				
Configuration items should be identified using established selection criteria.				
Configuration items should be selected whose functional and physical characteristics can be managed separately to achieve the overall end-use performance of the item.				
The number of configuration items selected should optimize the ability to control the product.				
The selection of configuration items should be initiated as early as possible in the product life cycle.				
The configuration items should be reviewed as the product evolves.				
5.3.3 Configuration baselines				
Configuration baselines should be established whenever it is necessary in the product life cycle to define a reference for further activities.				
5.5 Configuration status accounting				
5.5.1 General				
The organization should perform configuration status accounting activities throughout the life cycle of the product in order to support and enable an efficient configuration management process.				
5.5.2.2 The evolving product configuration information should be recorded in a manner that identifies the cross-references and interrelationships necessary to provide the required reports (see 5.5.3).				
5.6 Configuration audit				
Configuration audits should be performed in accordance with documented procedures to determine whether a product conforms to its requirements and product configuration information.				

10.2 Appendix B

CHECKLIST (Change)				
BS ISO 10007:2003	Santiago De Compostela			
	YES	**NO**	**N/A**	**I don`t know**
4.2 Dispositioning authority				
Did verify that the proposed change is necessary, and the consequences would be acceptable				
The change has been properly documented and categorized				
The planned activities for the implementation of the change into documents, hardware and/or software qwere satisfactory.				
5.4 Change control				
5.4.1 General				
After the initial release of product configuration information, all changes were controlled.				
The process for controlling the change was documented, and included the following:				
• a description of, justification for, and record of, the change;				
• a categorization of the change, in terms of complexity, resources and scheduling;				
• an evaluation of the consequences of the change;				
• details of how the change was dispositioned;				
• details of how the change was implemented and verified.				
5.4.2 Initiation, identification and documentation of the need for change				
Change proposals typically included the following information:				
• a description of the proposed change;				
• details of other configuration items or information that may be affected by the change;				
• the interested party preparing the proposal, and the date it was prepared;				
• the reason for the change;				
• the category of the change.				
The status of change processing, the related decisions and the dispositions were documented.				
5.4.3 Evaluation of change				
5.4.3.1 Evaluations concerning the proposed change were performed and documented. The extent of any evaluation was based on the complexity of the product, the category of the change , and should include the following:				
The technical merits of the proposed change				
The risks associated with the change				
The potential impact on contract, schedule and costs				
5.4.4 Disposition of change				
A process was established for the disposition of change that identifies the dispositioning authority (see 4.2) for each proposed change. This takes into account the category of the proposed change.				
The disposition was recorded. Notice of the disposition was circulated to relevant interested parties within and outside the organization.				
5.4.5 Implementation and verification of change				
After implementation, compliance with the approved change was verified. This verification was recorded to allow traceability.				