international Engineering Safety Management

Good Practice Handbook

Application Note 5

Some Examples of Estimating and Evaluating Risk

Published on behalf of the International Railway Industry
by Technical Programme Delivery Ltd – Issue 1 July 2014

We are grateful to the organizations listed who have supported iESM in various ways:

Disclaimer

Technical Programme Delivery Limited (TPD) and the other organizations and individuals involved in preparing this handbook have taken trouble to make sure that the handbook is accurate and useful, but it is only a guide. We do not give any form of guarantee that following the guidance in this handbook will be enough to ensure safety. We will not be liable to pay compensation to anyone who uses this handbook.

Acknowledgements

This Application Note has been written with help from the people listed below.

D Beacham
Dr G Bearfield
S Bickley
N Bowley
M Castles
P Cheeseman
Dr Chen Roger Lei
J-M Cloarec
Dr R Davis
B Elliott
T Jones
Dr KM Leung
Ms J Myde
Ng Nelson Wai Hung
G Parris
Sen Paul HB
Mrs Shi Lisa
A Russo
G Topham
Dr Fei Yan
Dr Zhang Simon

These people worked for the organizations listed below.

Abbot Risk Consulting
Arbutus Technical Consulting
Beijing National Railway Research and Design Institute of Signal and Communication Co. Ltd.
Beijing Traffic Control Technology Company
Bombardier Transportation
Certifer
Crossrail
EC Harris
Electrical and Mechanical Services Department, Hong Kong
Lloyd's Register
London Underground
MTR Corporation Limited, Hong Kong
RSSB, UK
Rio Tinto
Systra
Technical Programme Delivery Group

This guidance does not necessarily represent the opinion of any of these people or organizations.

Contents

1 Introduction

This Application Note is a component of the international Engineering Safety Management Good Practice Handbook, or 'iESM', for short. The handbook as a whole describes good practice in railway Engineering Safety Management (ESM) on projects. It covers both projects that build new railways and projects that change existing railways.

This handbook is structured in three layers (see right):

- Layer 1: Principles and process
- Layer 2: Methods, tools and techniques
- Layer 3: Specialized guidance

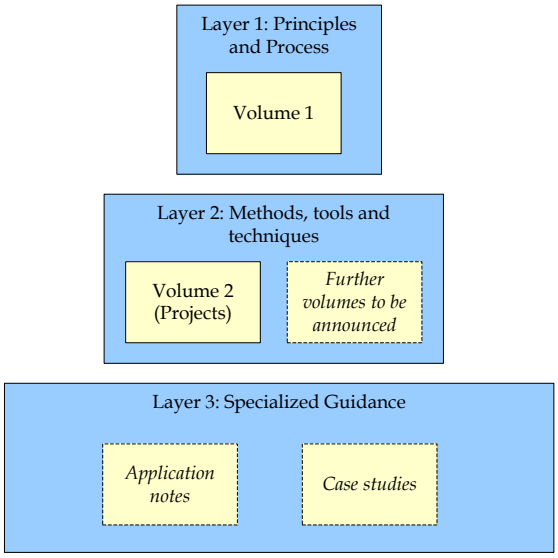

Figure 1. The structure of this handbook

The first layer comprises one volume, Volume 1. Volume 1 describes some of the safety obligations on people involved in changing the railway or developing new railway products. It also describes a generic ESM process designed to help discharge these obligations.

Volume 2 provides guidance on implementing the generic ESM process presented in Volume 1 on projects. Volume 2 belongs in the second layer. At the time of writing, Volume 2 was the only document in the second layer but further volumes may be added to this layer later

The third layer comprises a number of application notes providing guidance in specialized areas, guidance specific to geographical regions and case studies illustrating the practical application of the guidance in this handbook.

This document is Application Note 5. It supports the main body of the handbook by describing hypothetical examples of putting some of the guidance in volume 2 into practice. Figure 2 shows the generic ESM process which was introduced in volume 2 of the handbook with the parts of the process that this Application Note is designed to illustrate indicated with a red outline.

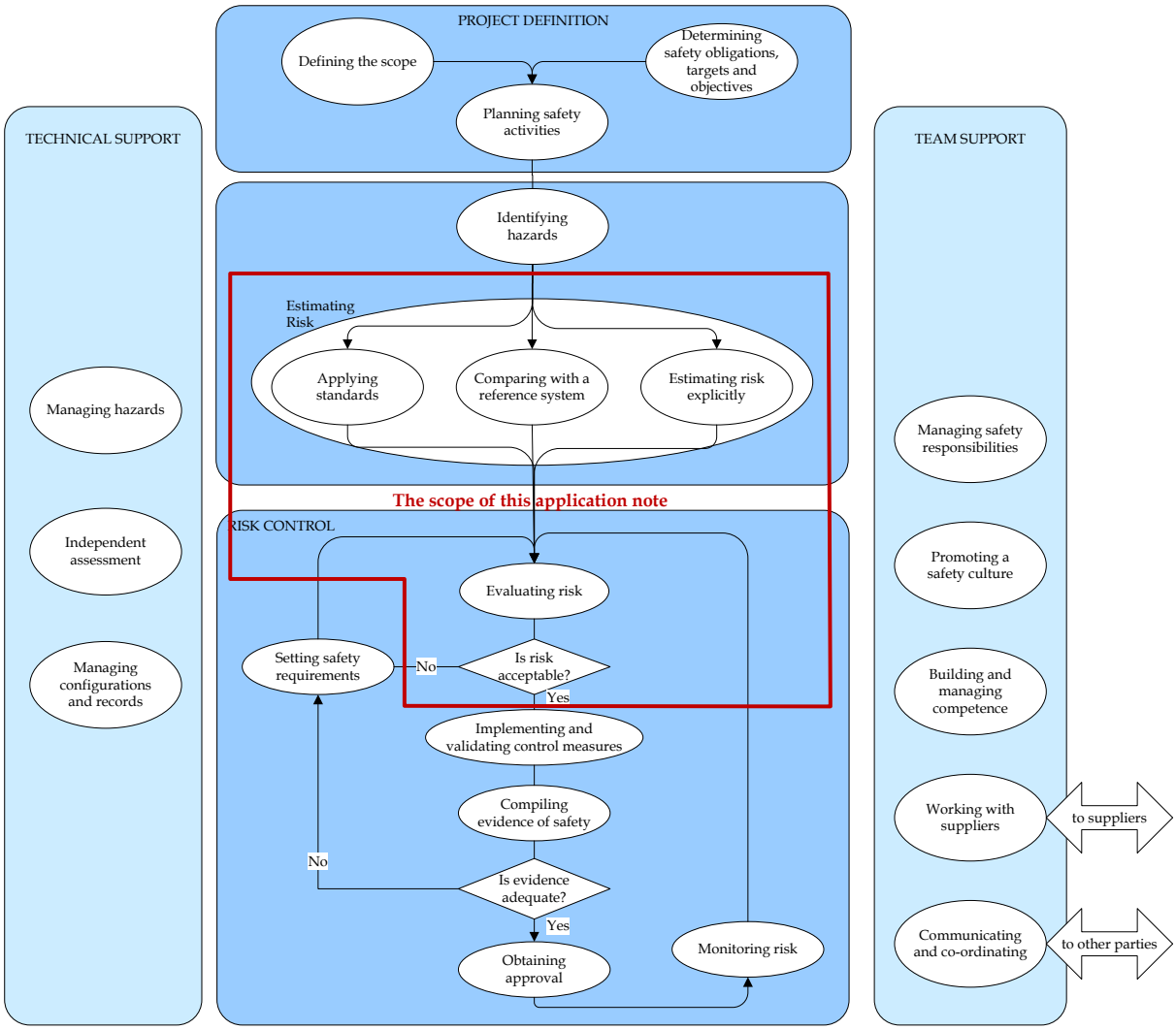

Figure 2. The scope of this Application Note

This Application Note provides examples of the processes of estimating risk and evaluating its acceptability, leading to the formulation of additional control measures and, all being well, to the decision that any residual risk is acceptable.

The examples are hypothetical and incomplete but are intended to be realistic examples of the sort of activities that may be carried out during risk estimation and evaluation.

If you have any comments on this Application Note or suggestions for improving it, we should be glad to hear from you. You will find our contact details on our web site, www.intesm.org. This web site contains the most up-to-date version of this Application Note. We intend to revise the handbook periodically and your comments and suggestions will help us to make the Application Note more useful for all readers.

2 The Hypothetical Example

iESM City is preparing to host a major international sporting event and is building a brand new stadium in disused docklands. iESM City has a metro network. In order to allow visitors to access the new stadium conveniently, the City Transit Authority (CTA) is extending the Blue Line to reach a new station, called Stadium (see below).

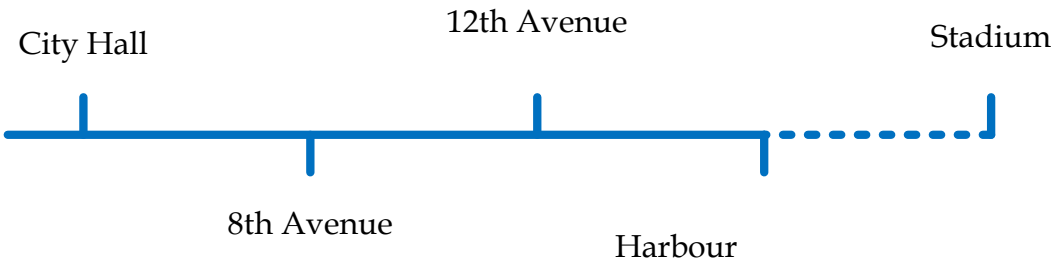

Figure 3. The Blue Line extension

The project under consideration is the extension of the line which includes:

- building Stadium station;
- extending the tunnel, using cut and cover methods to reach Stadium station;
- Additions to the track, power, signaling and telecommunications in order to extend the line through the tunnel to Stadium station; and
- procurement of 6 new trains, in order to increase peak service frequency.

The new trains are procured from the same supplier as the original trains and are almost identical to the original trains but there are two significant differences:

- The door controllers on the original trains use a processor which is no longer easily available and the supplier is providing new door controllers.
- While the saloons of the existing stock are lit by fluorescent lights, the salons of the new stock are lit by LED lights, which use less energy and require less maintenance.

The new infrastructure is generally constructed to the same standards as the existing infrastructure but Stadium station is built to carry greater flows of people than any other station on the line. In particular:

- All stations have escalators and lifts. While all existing stations have four escalators, arranged in two pairs (one up and one down) at opposite ends of the station, Stadium station has only one exit, leading to the sports facilities and the four escalators are arranged in a row and, at times of peak flow, can be set up with three carrying people in one direction and one in the other direction.

3 Preparatory Activities

This Application Note provides examples of activities to estimate and evaluate risk. There are three activities in the generic ESM process that provide input to estimating and evaluating risk, as depicted below:

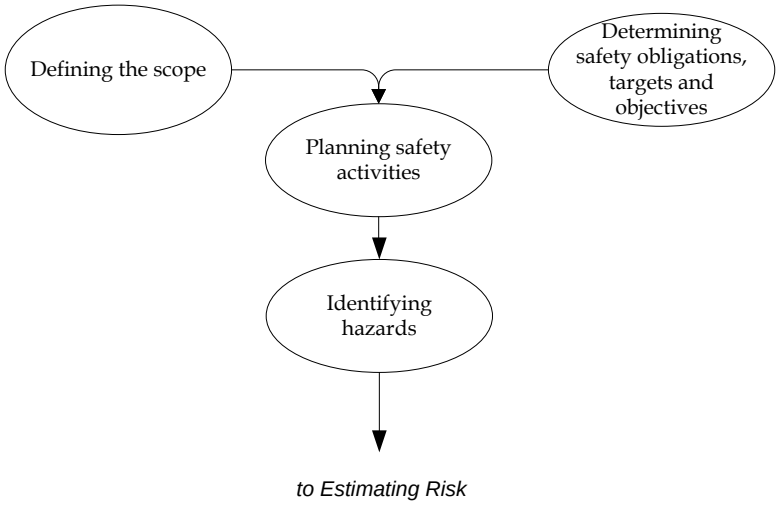

Figure 4. Preparatory activities

We do not describe these activities but we do describe the outputs from these activities, which are inputs to estimating and evaluating risk.

3.1 Output from the 'Defining the scope' activity

The output from this activity is:

- a definition of the Stadium Extension, encompassing everything that needs to be created or changed, including operational and maintenance procedures as well as physical assets; and
- a definition of relevant aspects of the environment in which the Stadium Extension will operate, including interfaces with the rest or the world and contextual information such as estimated passenger numbers.

The arrows in the flow chart for the generic ESM process do not indicate that the activity at the tail of the arrow must finish before the activity at the head of the arrow can start: there is generally some iteration.

The scope of the project is defined in increasing detail the early stages of the project. Work starts on estimating risk before the scope is fully defined.

Before the start of preliminary hazard analysis (see the next chapter), which is the first stage of risk estimation, the following are prepared:

- a requirements specification for the project;
- a top-level system design for the extension;
- outline specifications for the major sub-systems of the project including the tunnels, track, trains, train control, stations and electrification;
- definitions of the major interfaces between the major sub-systems;
- definitions of the major interfaces that the Stadium Extension has with external systems; and
- an operational concept, including timetables and estimates of average and peak passenger flows.

Before detailed risk estimation is started, the material above is supplemented with detailed designs for the extensions and its components.

3.2 Output from the 'Determining safety obligations, targets and objectives' activity

The output of this activity is a statement of the safety obligations, targets and objectives that the project must meet.

CTA has a legal obligation to ensure that significant changes that it makes to its metro system do not degrade safety. CTA has well-defined generic safety objectives for changes to the metro system and these are consistent with this legal obligation.

This activity confirms that the generic safety objectives are applicable to the Stadium Extension. CTA's principal safety objective for the Stadium Extension, like any other project, is that:

- the project shall not increase the overall risk of death of injury faced by a typical CTA passenger, CTA worker or CTA neighbor.

CTA maintains a quantified risk model which is used to calculate estimates of these risks from estimates of the rates of occurrence of hazards and other events and from passenger and traffic volumes.

CTA's procedures require that full risk estimation and evaluation should be preceded by a preliminary hazard analysis in which the risk associated with each hazard is assessed using the likelihood-severity matrix reproduced in Table 1.

A risk in the 'Unacceptable' would be higher than the levels of risk currently experienced on the metro system and therefore would be inconsistent with the principal safety objective for the project. If the risk associated with a hazard falls into the 'Unacceptable' area then it must be reduced before the project can proceed.

A risk in the 'Negligible' area would be negligible in comparison with the levels of risk currently experienced on the metro system and therefore would not have to be

reduced in order to meet the principal safety objective for the project. If the risk associated with a hazard falls into the 'Negligible' area then it may be accepted without further risk estimation and evaluation.

The 'Possibly Acceptable' area lies between the 'Unacceptable' and 'Negligible' areas. If the risk associated with a hazard falls into the 'Possibly Acceptable' area then further risk estimation and evaluation is required as described below the table.

Note. The legal obligations, corporate targets and project objectives have been invented for the purposes of the example. Your safety obligations, targets and objectives will be different from those in the example and you will have to select risk evaluation methods that are appropriate to your context. Even if your safety obligations, targets and objectives are similar to those in the example, you may choose to use different risk evaluation methods. It is, for instance, possible to show that the legal obligation listed above has been met without using a likelihood-severity matrix.

Readers who are used to a legal obligation to reduce risk to a level which is as low as reasonably practicable may have used similar matrices but should note that, in this example, a different legal framework is being used and the matrix is not being used to support a decision about what is and is not reasonably practicable.

Table 1. Likelihood-severity matrix used by CTA for preliminary hazard analysis

Likelihood	Severity			
	Minor Minor injuries only	**Major** Major injuries, not fatalities	**Critical** Single fatality	**Catastrophic** Multiple fatalities
High > once per month	Unacceptable	Unacceptable	Unacceptable	Unacceptable
Medium < once per month > once per year	Possibly Acceptable	Possibly Acceptable	Unacceptable	Unacceptable
Low < once per year > once per 10 years	Possibly Acceptable	Possibly Acceptable	Possibly Acceptable	Unacceptable
Very Low < once per 10 years > once per 100 years	Negligible	Possibly Acceptable	Possibly Acceptable	Possibly Acceptable
Extremely Low < once per 100 years	Negligible	Negligible	Negligible	Negligible

When the risk falls into the 'Possibly Acceptable' area, CTA uses risk estimation and evaluation processes which are similar to those defined in the European Common Safety Method on Risk Estimation and Acceptance [CSM-REA]. The risk associated with a hazard may be accepted if one of the following holds:

1. **Existing standards.** The risk is completely covered by existing CTA standards and/or international standards adopted by CTA and there are no significant and relevant differences between the circumstances in which the risk occurred and the circumstances anticipated when the standard was written.
2. **Reference system.** The risk is no greater than that associated with equipment, systems or processes which:
    - have similar functions and interfaces;
    - are operated in similar operational end environmental conditions; and
    - have been accepted for use on the iESM City metro or a named list of other metros with similar safety records and scopes of operation.
3. **Explicit risk assessment**. The risk is estimated quantitatively and found to meet one of two criteria:

- **The absolute risk acceptance criterion.** CTA adopts the risk acceptance criterion stated in the European Union Common Safety Method on Risk Evaluation and Acceptance that '*For technical systems where a functional failure has credible direct potential for a catastrophic consequence, the associated risk does not have to be reduced further if the rate of that failure is less than or equal to 10^{-9} per operating hour*'.
- **The comparative risk acceptance criterion.** The risk assessment shows that the change being made by the railway will not increase the overall risk of death of injury faced by a typical CTA passenger, CTA worker or CTA neighbor.

The risk assessment processes are listed in an order of precedence. A process from the list above should not be used unless it is impractical to take all lower-numbered options. CTA requires that the rationale for selecting a risk estimation and evaluation process should be recorded.

Note. Risk evaluation leads to a judgement on whether or not the risk is acceptable but does not include the final acceptance of the risk, which occurs during the ***Obtaining approval*** *activity in Figure 2 and is outside the scope of this Application Note.*

3.3 Output from the 'Planning safety activities' activity

The output from this activity is a Safety Plan for the project. The Safety Plan defines the risk estimation and evaluation activities that are carried out but does not contain information (other than the outputs from the 'Defining the scope' and 'Determining safety obligations, targets and objectives' activities) that is input to risk estimation and evaluation and so is not discussed further.

3.4 Output from the 'Identifying hazards' activity

This activity delivers a list of hazards for the Stadium Extension. A systematic search is made for all hazards associated with the Stadium Extension and its interfaces with the rest of the world

CTA maintains a Hazard Log for the Blue Line, which contains information about hazards of the major sub-systems of the line in a large database table. Table 2 contains an extract from the Hazard Log showing only a few of the hazards and omitting some of the columns.

The hazards in the Blue Line Hazard Log are all included within CTA's risk model, from which quantitative estimates of the rate of occurrence of each hazard and the consequences may be obtained. The Blue Line Hazard Log contains qualitative estimates of likelihood and severity of an accident associated with each hazard after allowance for the effect of the control measures listed. These estimates are conservative but not the worst case – they represent consensus judgment on the

highest values from the plausible range of values that might be associated with the hazard.

Note. The estimates of likelihood and severity in the Blue Line Hazard Log concern the existing Blue Line. They are not necessarily valid for the Stadium Extension and they are reviewed and, where necessary, revised before being incorporated into the Stadium Extension Hazard Log, as described in the next section.

A multi-disciplinary team, including engineers, operators and maintainers is convened to identify hazards associated with the Stadium Extension. The team reviews the Blue Line Hazard Log and decides whether each hazard is relevant to the extension or not. Then the team carries out a structured brainstorm during which they consider:

- each major hardware and software component of the Stadium Extension;
- each major interface associated with the Stadium Extension; and
- each significant operational or maintenance change associated with the Stadium Extension.

The team looks for additional hazards which the Stadium Extension might introduce. A few additional hazards are identified including the following:

Subsystem	**Sub-sub-system**	**Hazard**	**Consequences**
Stations	Escalators	A large flow of passengers arriving within a short period of time from the stadium at the end of an event results in overcrowding of the ground floor ticket hall or the lobby at the foot of the escalator.	Possibility that several passengers on the escalator will be knocked over, in which case multiple serious injuries and fatalities might arise. Possibility of multiple serious injuries and fatalities arising from crushing at foot of escalator.

Table 2. Extract from the Hazard Log for the Blue Line

Subsystem	Sub-sub-system	Hazard	Control measures	Severity	Likelihood
…	…	…	…	…	…
Trains	Doors	Door controller allows application of traction power with door open	• The door release and traction enable functions of the door controller are designed and constructed to achieve safety integrity of SIL 4. • Duplicated detection arrangements. • Door controllers perform self-test on power up. • Lock status detectors inspected every week. • Operational procedures require any train with a failed door to be withdrawn from service.	Critical	Very low
Trains	Doors	EMI from door controller interferes with other train control systems	• Door controller certified against EN50121-3-2, 'Rolling stock – Apparatus'. • Door controller tolerance of EMI tested according to CTA standards.	Critical	Very low
…	…	…	…	…	…

Subsystem	Sub-sub-system	Hazard	Control measures	Severity	Likelihood
Trains	Saloon lighting	Potential for electrocution of maintenance technician working on saloon lighting	• Maintenance technicians are trained, competent and supervised. • Maintenance procedures require that the power supply to the saloon lighting should be interrupted before the cover is opened.	Critical	Very low
Trains	Saloon lighting	Potential for fire in saloon lighting	• Saloon lighting circuits are protected by circuit breakers.	Catastrophic	Very low
…	…	…	…	…	…
Stations	Escalators	Congestion at exits from escalator prevents people on the escalator from leaving when they reach the exit leading to slips, trips or crushing	• The exits from escalators are monitored by CCTV and operational procedures require intervention if congestion starts to build.	Catastrophic	Very low
Stations	Escalators	Escalator stops suddenly	• Escalator construction, installation, testing and maintenance must meet CTA standards. • Escalators are designed to come to a controlled and gradual halt if power is interrupted.	Catastrophic	Very low
…	…	…	…	…	…

Subsystem	Sub-sub-system	Hazard	Control measures	Severity	Likelihood
Stations	Lobbies, corridor and platforms	Slippery floor surface	• CTA standards require that the floor surfaces should have non-slip properties, even when wet. • CTA operational standards require that lobbies, corridor and platforms should be regularly monitored by station staff, directly or via CCTV, and station staff are required to react promptly to any spillages and cordon off the affected areas until the spillage has been dealt with.	Minor	Medium
…	…	…	…	…	…
Track	-	Broken rail	• Rigorous testing and inspection of rail is required before installation. • Inspections are carried out according to maintenance procedures specify frequency and nature of inspections. • Maintenance procedures set criteria for the imposition of a temporary speed restriction and emergency repairs.	Catastrophic	Very low
…	…	…	…	…	…

4 Preliminary Hazard Analysis

The guidance on risk estimation in chapter 8 of volume 2 of the iESM Handbook, includes the following points:

c. If you are delivering a system or product, you should carry out a preliminary hazard analysis early in the project.

d. If you are delivering a system or product, you should decide upon your approach to risk estimation early in the project.

In accordance with this guidance and with its own internal procedures, the CTA Stadium Extension project team carries out a Preliminary Hazard Analysis before detailed design starts.

The team establishes a project Hazard Log and copies into it the existing Blue Line hazards which were found to be applicable and the new hazards which were found to be associated with the extension.

A multi-disciplinary team, including engineers, operators and maintainers is convened to review this Hazard Log. The team is chosen to provide the range of competences required to perform a thorough review and is thoroughly briefed about the CTA preliminary hazard analysis process.

During this process, the team considers each hazard in the context of the Stadium Extension. Where possible, they use the information from the existing Blue Line Hazard Log as a starting point but consider whether it remains valid for Stadium Extension. They review:

- The causes of the hazard. For instance, causes of 'Escalator stops suddenly' include mechanical failure and power failure.
- The consequences of the hazard. For instance, consequences of 'Escalator stops suddenly' include falls for one or more of the passengers standing on the escalator and, when the escalator is fully loaded, a potential cascade leading to all occupants falling.
- The control measures for the hazard. For instance, control measures for 'Escalator stops suddenly' include the facts that escalator construction, installation, testing and maintenance must meet CTA standards and that escalators are designed to come to a controlled and gradual halt if power is interrupted.

The team then reaches consensus judgment on the severity and likelihood classes for each hazard on the Stadium Extension after taking into account the effect of the control measures. As for the Blue Line Hazard Log, these estimates are conservative but not the worst case – they represent consensus judgment on the highest values from the plausible range of values that might be associated with the hazard.

The team also decides which of the three methods of risk estimation and evaluation ('Existing standards', 'Reference system' and 'Explicit risk assessment'– see section 3.2 above) is appropriate for each hazard. As described in section 3.2 above, the methods are considered in the order listed and the first applicable technique is used.

The conclusions of the preliminary hazard analysis are recorded in a preliminary hazard analysis report. This report contains a comprehensive account of the process followed, the personnel involved, the conclusions reached and the rationale for reaching these conclusions. The key facts relating to hazards are copied from this report into the project Hazard Log. Table 3 contains extracts from this Hazard Log.

Table 3. Extract from the Hazard Log for the Stadium Extension project after Preliminary Hazard Analysis

Subsystem	Sub-sub-system	Hazard	Control measures	Severity	Likelihood	Risk Estimation Method
…	…	…	…	…	…	
Trains	Doors	Door controller allows application of traction power with door open	• The door release and traction enable functions of the door controller are designed and constructed to achieve safety integrity of SIL 4. • Duplicated detection arrangements. • Door controllers perform self-test on power up. • Lock status detectors inspected every week. • Operational procedures require any train with a failed door to be withdrawn from service.	Critical	Very low	Explicit risk assessment *(No applicable standards and no reference system available.)*
Trains	Doors	EMI from door controller interferes with other train control systems	• Door controller certified against EN50121-3-2, 'Rolling stock – Apparatus'. • Door controller tolerance of EMI tested according to CTA standards	Catastrophic	Very low	Existing standards
…	…	…	…	…	…	

Subsystem	Sub-sub-system	Hazard	Control measures	Severity	Likelihood	Risk Estimation Method
Trains	Saloon lighting	Potential for electrocution of maintenance technician working on saloon lighting	• Maintenance technicians are trained, competent and supervised. • Maintenance procedures require that the power supply to the saloon lighting should be interrupted before the cover is opened. • Lighting luminaires for the new train will use low-voltage LEDs and are powered by 12V DC external suppliers.	Critical	Extremely low[1]	*No further risk estimation is required because the severity and likelihood place the risk in the 'Negligible' area.*
Trains	Saloon lighting	Potential for fire in saloon lighting	• Saloon lighting circuits are protected by circuit breakers.	Critical	Very low	Reference system *(No applicable standards.)*
…	…	…	…	…	…	

[1] The reduction in supply voltage allowed by LEDs results in this hazard having a lower likelihood for the new trains than the old ones. The combination of failures required to allow 240V to be fed to the luminaires and then for an electrocution to occur is considered to be extremely unlikely.

Subsystem	Sub-sub-system	Hazard	Control measures	Severity	Likelihood	Risk Estimation Method
Stations	Escalators	Congestion at exits from escalator prevents people on the escalator from leaving when they reach the exit	• The exits from escalators are monitored by CCTV and operational procedures require intervention if congestion starts to build. • Emergency stop buttons are placed adjacent to the escalators.	Catastrophic	Low	Reference system *(No applicable standards.)*
Stations	Escalators	Escalator stops suddenly	• Escalator construction, installation, testing and maintenance must meet CTA standards. • Escalators are designed to come to a controlled and gradual halt if power is interrupted.	Catastrophic	Very low	Existing standards
Stations	Escalators	A large flow of passengers arriving within a short period of time from the stadium at the end of an event results in overcrowding of the ground floor ticket hall or the lobby at the foot of the escalator.	• The ground floor ticket halls is monitored by CCTV and operational procedures require intervention if congestion starts to build.	Catastrophic	Low	Reference system *(No applicable standards.)*
…	…	…	…	…	…	

Subsystem	Sub-sub-system	Hazard	Control measures	Severity	Likelihood	Risk Estimation Method
Stations	Lobbies, corridor and platforms	Slippery floor surface	• CTA standards require that the floor surfaces should have non-slip properties, even when wet. • CTA operational standards require that lobbies, corridor and platforms should be regularly monitored by station staff, directly or via CCTV, and station staff are required to react promptly to any spillages and cordon off the affected areas until the spillage has been dealt with.	Minor	Medium	Existing standards
…	…	…	…	…	…	…
Track	-	Broken rail	• Rigorous testing and inspection of rail is required before installation. • Inspections are carried out according to maintenance procedures which specify frequency and nature of inspections. • Maintenance procedures set criteria for the imposition of a temporary speed restriction.	Catastrophic	Very low	Existing standards
…	…	…	…	…	…	

5 Risk Estimation and Evaluation

This section contains a description of the risk estimation and evaluation activities leading to a decision regarding the acceptability of the risk associated with a sample of hazards. The decision in all cases is that the risk is acceptable but, in some cases, additional control measures are formulated before that decision can be reached.

The hazards considered are grouped according to the major sub-system to which they relate: trains, stations and track.

This Application Note only includes a summary of the output from these activities. Comprehensive records of the risk estimation and evaluation process are maintained by the Stadium Extension project team, including records of the process followed, the personnel involved, calculations performed, assumptions made and the rationale for the conclusions reached.

5.1 Risk Estimation and Evaluation - Trains

5.1.1 Door controller allows application of traction power with door open

The risk associated with this hazard is estimated and evaluated by explicit risk assessment using the absolute risk acceptance criterion, that is by showing that the rate of the failure causing the hazard is less than or equal to 10^{-9} per operating hour.

Risk Estimation

Figure 1 below presents a partial block diagram for the door controller and associated equipment, restricted to those components related to detecting door status.

Each door is fitted with a door controller. When closed, the door is held in position by two locks and the status of each lock is sensed by a detector. The door controller is a redundant computerised system with two independent controllers. When each controller receives input that both locks are locked, it closes a relay on the train traction control line. Traction power cannot be applied unless all these relays are closed.

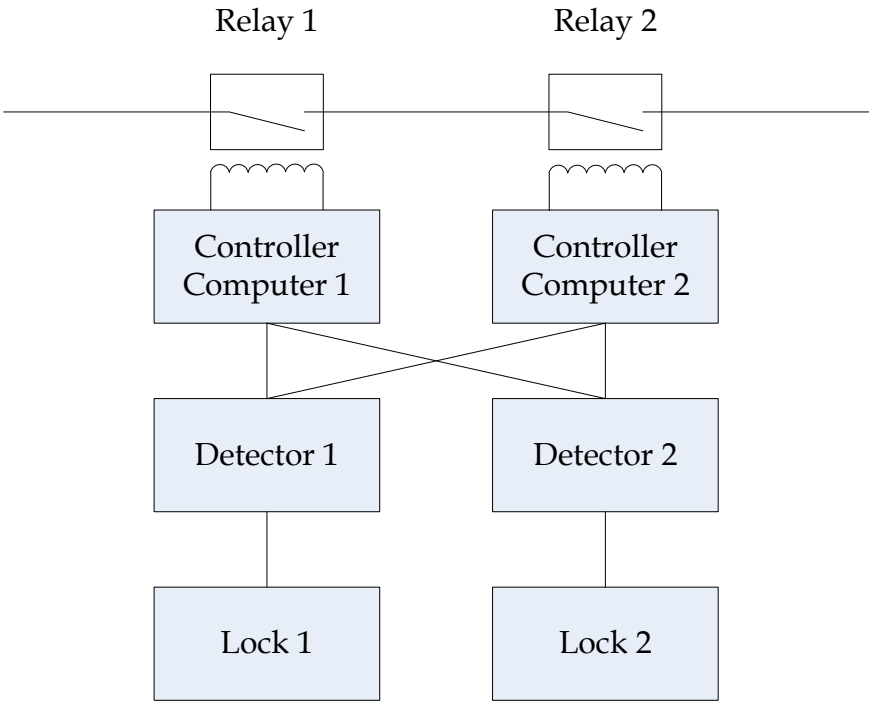

Figure 5. Partial block diagram for door controller

The method used to show that the target rate of occurrence of the hazard is achieved is consistent with the guidance provided in volume 2 of the iESM Handbook and in EN 50129 [50129]:

- It is shown, using fault tree analysis that the rate of random failures, which in the case of the door controller means hardware failures, is is less than or equal to 10^{-9} per operating hour.
- Recognizing all systematic failures of the door controller are failures of t he embedded software, it is shown that the software has been developed to deliver a safety integrity of SIL 4 for the traction interlocking function, an integrity which is commensurate with this target (see chapter 9 of volume 2 of the iESM Handbook).

Figure 6, below, shows a fault tree for the hazard under consideration. Fault tree analysis is a formal technique for causal analysis. The fault tree indicates the combination of events which may cause the hazard. For further description of the fault tree notation, see Application Note 3.

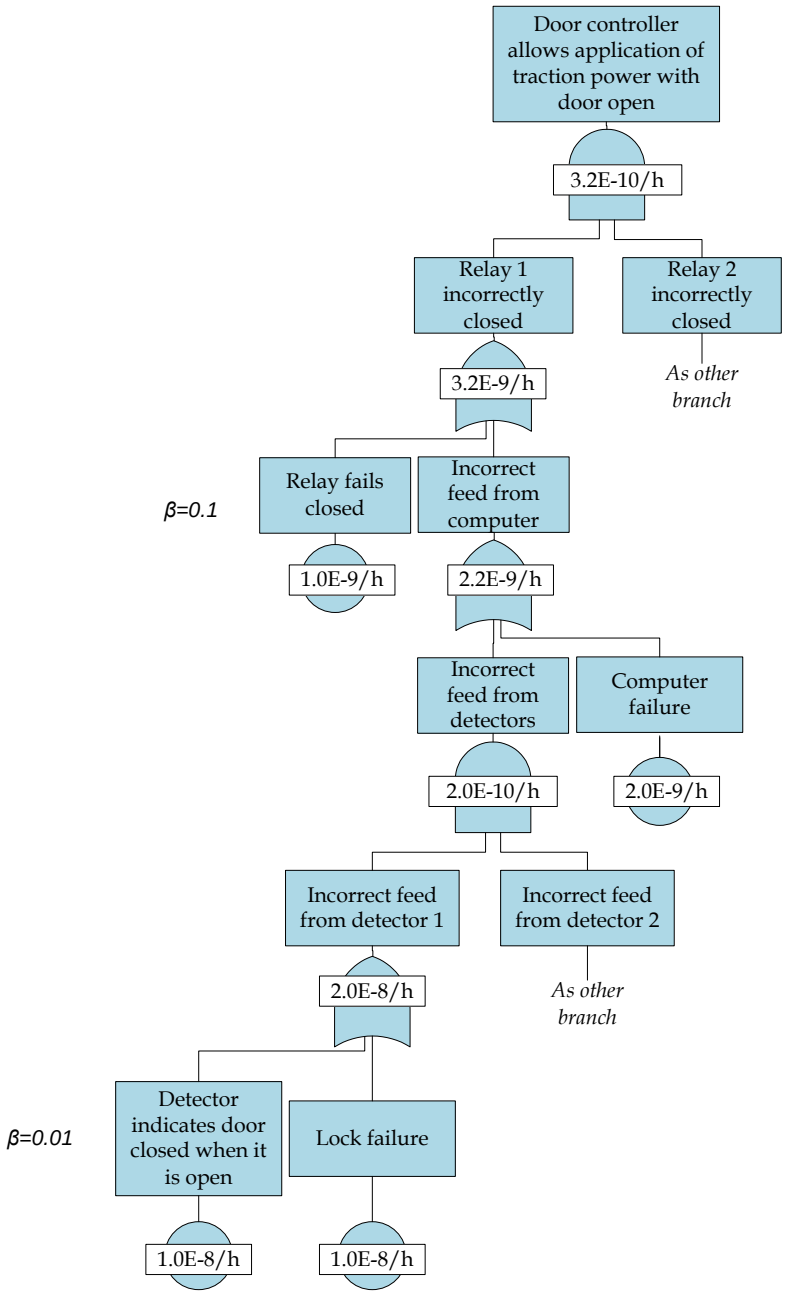

Figure 6. Fault tree for the hazard, 'Door controller allows application of traction power with door open'

The fault tree is annotated with estimates of the rates of occurrence of the events. The new door controller shares some components with the door controller on existing stock. Failure rates for these components are taken from statistics collected by CTA about the failure rates in the field. CTA has accumulated these statistics over a significant period and after reviewing the guidance on use of historical data in section 8.2.9 of iESM volume 2, they are considered to be a sound basis for

extrapolation. Failure rates for the new component are taken from manufacturer's figures because CTA has no experience of the failure rate of this component. It is noted that the fault tree rests on the assumption that the manufacturer's figure for the failure rate of this component proves to be achieved in the CTA application. Nominal estimates are used in the fault tree but worst case estimates are also made for sensitivity analysis (see later).

The calculation of the rate of occurrence some events takes account of correlation between the causes of the event.

Note. The annotations of the form 'β=…' indicate that an allowance is being made for correlation.

The estimated frequency with which the hazard will occur as a result of random failure is 3.2×10^{-9} per operating hour. There is uncertainty in some of the estimates for the frequency of occurrence of the causes and so a sensitivity analysis is carried out which suggests that the frequency of occurrence of the hazard as a result of random failure is between 2.0×10^{-9} per operating hour and 4.2×10^{-9} per operating hour.

It is shown that the software of the controller has been developed according to the requirements of SIL 4, in EN 50126-1:1999 [50126] and it follows that the integrity of the traction interlocking function is SIL 4.

Risk Evaluation

The estimated rate of occurrence for the hazard has been shown to be less than 10^{-9} per operating hour under worst-case assumptions and so the risk is considered to be acceptable, subject to confirmation that the assumption that the manufacturer's figure for the failure rate of the new door controller component proves to be achieved in the CTA application, which is to be confirmed by monitoring failures of this component for the first six months of operation.

5.1.2 EMI from door controller interferes with other train control systems

The risk associated with this hazard for the new controller is estimated and evaluated by use of existing standards, on the basis of:

- certification of the controller against EN 50121-3-2, 'Rolling stock – Apparatus' [50121-3-2]; and
- testing of the controller according to CTA standards which require demonstration that it functions correctly in the presence of the worst case EMI found on the metro system.

Note. When using the 'Existing standards' process for estimating and evaluating risk, risk estimation and risk evaluation are not distinct activities – the two are performed at the same time.

EN 50121-3-2 had been adopted by CTA these standards were used to accept the risk associated with this hazard for the previous controller.

The controller is required to be certified against this standard by an independent test house – a process which requires inspections and tests to be performed at the supplier factory and on the Blue Line.

The risk is considered to be acceptable, subject to receipt of the required certificate.

5.1.3 Potential for fire in saloon lighting

The risk associated with this hazard is estimated and evaluated by comparison with a reference system because CTA does not yet have standards for fire safety of LED lighting.

Risk Estimation

The previous fluorescent lighting for the rolling stock, meet the criteria for use as a reference system set out in section 3.2 because it:

- has similar (in fact, identical) functions and interfaces;
- is operated in similar (in fact, identical) operational end environmental conditions; and
- has been accepted for use on the iESM City metro.

The previous fluorescent lighting for the rolling stock is used as a reference system.

A comparison of the new LED lighting with the previous fluorescent lighting reveals that:

- the normal operating temperature of the LED lights is lower than that of the fluorescent lights;
- the voltages in an LED luminaire are lower than in a fluorescent luminaire; and
- the electrical power drawn and the maximum electrical power available are lower for an LED luminaire than for a fluorescent luminaire.

Risk Evaluation

As there are no other significant differences between the fluorescent and LED lighting arrangements and there are no known high-temperature failure modes of the LED lights, it is concluded that the risk of fire starting in the LED saloon lighting is lower than the risk of the same hazard for the existing fluorescent lighting. As the latter risk was and remains acceptable, it is considered that the risk associated with this hazard is acceptable.

5.2 Risk Estimation and Evaluation - Stations

5.2.1 Congestion at exits from escalator prevents people on the escalator from leaving when they reach the exit AND Overcrowding of the ground floor ticket hall

These two hazards are considered together because the control measures that are effective against them overlap.

The risk associated with these hazards is estimated and evaluated by comparison with reference systems.

Risk Estimation

The project team reviews the standard measures that are in place on the Blue Line to prevent escalator accidents arising from overcrowding. They are:

- The exits from escalators are monitored by CCTV and operational procedures require intervention if congestion starts to build.
- Emergency stop buttons are placed adjacent to the escalators.

The project team cannot conclude that these standard control measures are sufficient at Stadium station because the passenger flows and escalator layouts at Stadium station are not experienced elsewhere on CTA network and were not contemplated when the standard control measures were drawn up.

The general circumstances that will be encountered at Stadium station are however encountered on a station in another metro with a similar safety record. The escalators at this station meet the criteria for use as a reference system set out in section 3.2 because

- they have similar functions and interfaces;
- they are operated in similar operational end environmental conditions; and
- the metro is on a named list of other metros with safety records and scopes of operation that are similar to CTA's metro system.

The escalator in the station in the other metro is used as a reference system.

CTA carries out a review of the measures in place on at this station and concludes that taking the following additional control measures at Stadium station would reduce risk to a level no higher than that encountered elsewhere:

- At peak periods, staff, in radio contact with station control, should be assigned to monitor the areas adjacent to the top and bottom of the escalators and to direct infirm passengers to the lifts.
- At periods of peak flow of passengers into the station from the stadium, the escalators should be turned off and used as stationary staircases, in order to reduce the risk of overcrowding leading to crush or fall injuries.

Note. Under most circumstances, CTA considers that risk is increased by switching off escalators. However analysis of the experience at the reference station shows that, in the situation where a very large number of passengers reaches the station from the stadium, this measure provides better control of the flow of passengers and reduce risk.

- Entry and exit routes through the station should be separated and clearly marked.
- Temporary barriers should be procured which can be erected at the foot of the escalators to segregate the two flows of passengers for a distance of 4 meters
- The external doors to the station should be designed in a manner which allows station staff to close the entrance to the station (while leaving the exit clear) quickly if this is necessary to prevent dangerous overcrowding.
- A covered walkway to the station should be provided so that passengers do not linger in the station foyer to put up umbrellas when it is raining.

Risk Evaluation

Having concluded that the risk after taking these measures is no higher than levels which are accepted on the reference system, the risk associated with these hazards is considered to be acceptable, subject to satisfactory implementation of the defined control measures.

5.2.2 Escalator stops suddenly

The risk associated with this hazard is estimated and evaluated by use of existing standards.

The standards to which the escalators at Stadium station are constructed and maintained are the same as for other stations. These standards are intended to be sufficient for periods when the escalators are fully loaded and there are no significant differences which affect the risk and so the risk associated with the hazard is considered to be acceptable with reference to these standards.

5.2.3 Slippery floor surface

The risk associated with this hazard is estimated and evaluated by use of existing standards.

The standards to which the floor surface at Stadium station is constructed and the standards for operational response to spillages are the same as for other stations. There are no factors which significantly alter the risk of this hazard at Stadium station and so the risk associated with the hazard is considered to be acceptable with reference to these standards.

5.3 Risk Estimation and Evaluation - Track

5.3.1 Broken rail

The risk associated with this hazard is estimated and evaluated by use of existing standards.

CTA's track standards require rigorous testing and inspection of rail is required before and immediately after installation.

CTA's track maintenance standards require rigorous testing and inspection of rail is required before installation specify the frequency and nature of track inspections and set criteria for the imposition of a temporary speed restriction.

The standards to which new track is constructed and maintained are the same as for existing track and there are no significant differences which affect the risk on the Stadium Extension and so the risk associated with the hazard is considered to be acceptable with reference to these standards.

6 Follow-up Activities

This section briefly describes what happens how the results of risk estimation and evaluation are used in order to support the delivery of a safe system. Figure 7, below, shows the activities in the generic ESM process to which estimating and evaluating risk directly contribute.

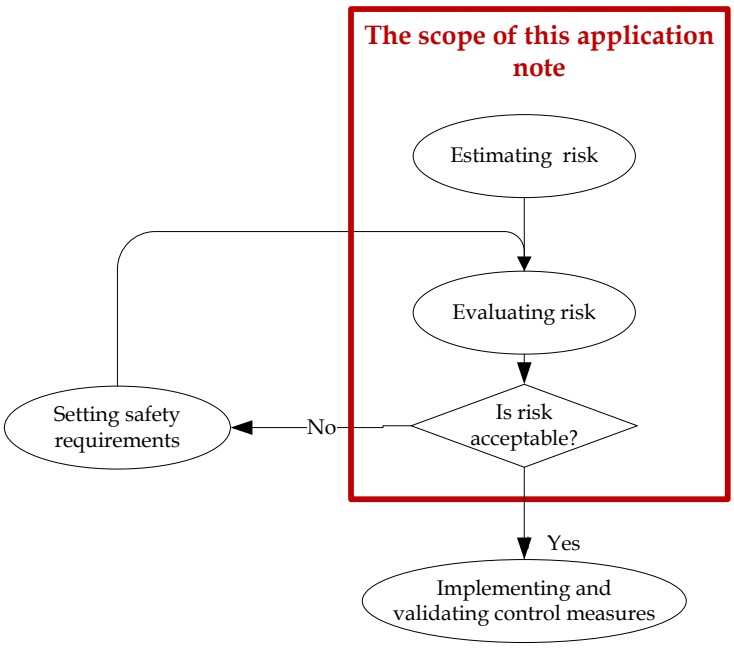

Figure 7. Follow-up activities

During the process of estimating and evaluating risk, all control measures which have were assumed or were found to be necessary are recorded as safety requirements.

Table 4 provides simplified versions of these safety requirements (the actual safety requirements are longer and worded more precisely).

These safety requirements are then allocated to the relevant CTA team or contractor. Validation activities are defined and performed to confirm that all safety requirements have been implemented.

Table 4. Sample safety requirements for the Stadium Extension project after Preliminary Hazard Analysis

Subsystem	Sub-sub-system	Hazard	Simplified safety requirements
…	…	…	…
Trains	Doors	Door controller allows application of traction power with door open	• The door release and traction enable functions of the door controller shall be designed and constructed to achieve safety integrity of SIL 4. • Two independent detectors shall be used to confirm that each door is locked. • The door controller software shall carry out a self-test after start up. • Operational procedures shall ensure that any train with a failed door is immediately withdrawn from service.
Trains	Doors	EMI from door controller interferes with other train control systems	• The door controller shall be certified against EN50121-3-2, 'Rolling stock – Apparatus' • The door controller's tolerance of EMI shall by confirmed by testing according to CTA standards
…	…	…	…
Trains	Saloon lighting	Potential for electrocution of maintenance technician working on saloon lighting	• Maintenance procedures shall require that technician maintaining trains are trained, competent and supervised. • Maintenance procedures shall require that the power supply to the saloon lighting be interrupted before the luminaire cover is opened. • Lighting luminaires shall use low-voltage LEDs and shall be powered only by 12V DC external suppliers.
Trains	Saloon lighting	Potential for fire in saloon lighting	• Saloon lighting circuits shall be protected by circuit breakers.
…	…	…	…

Subsystem	Sub-sub-system	Hazard	Simplified safety requirements

Stations	Escalators	Congestion at exits from escalator prevents people on the escalator from leaving when they reach the exit	• Operational procedures at Stadium station shall require that:
			  ○ the exits from escalators be monitored by CCTV and shall require intervention if congestion starts to build;
			  ○ at peak periods, staff, in radio contact with station control, should be assigned to monitor the areas adjacent to the top and bottom of the escalators and to direct infirm passengers to the lifts; and
			  ○ at periods of peak flow of passengers into the station from the stadium, the escalators should be turned off and used as stationary staircases.
			• Entry and exit routes through Stadium station shall be separated and clearly marked.
			• Temporary barriers shall be procured and stored at Stadium station which can be erected at the foot of the escalators to segregate the two flows of passengers for a distance of 4 meters.
			• The external doors to Stadium station should be designed in a manner which allows station staff to close the entrance to the station (while leaving the exit clear) quickly if this is necessary to prevent dangerous overcrowding.
			• A covered walkway to Stadium station should be provided so that passengers do not linger in the station foyer to put up umbrellas when it is raining.
			• Emergency stop buttons shall be placed adjacent to the escalators as required by CTA standards.

Stations	Escalators	A large flow of passengers arriving within a short period of time from the stadium at the end of an event results in overcrowding of the ground floor ticket hall or the lobby at the foot of the escalator.	
Stations	Escalators	Escalator stops suddenly	• Escalators shall be constructed, installed, maintained and tested according to CTA standards. • Escalators shall be designed to come to a controlled and gradual halt if power is interrupted.
…	…	…	…

Subsystem	Sub-sub-system	Hazard	Simplified safety requirements
Stations	Lobbies, corridor and platforms	Slippery floor surface	• The floor surfaces shall be constructed according to CTA standards. • Surveillance of station areas and response to spillages should be carried out according to CTA standards.
…	…	…	…
Track	-	Broken rail	• Rail shall be installed and maintained according to CTA standards
…	…	…	…

7 Conclusions

This example has been provided in order to illustrate the application of ESM methods. The example is simplified and based up on assumptions that are unlikely to hold in your application. It is unlikely that any of the details of this example can be used without change in another application – the underlying methods would have to be applied afresh.

8 Glossary

This glossary defines the specialized terms and abbreviations used in this Application Note.

8.1 Abbreviations

CCTV	Closed Circuit Television
CTA	The City Transit Authority of the fictitious iESM City
EMI	Electromagnetic Interference
ESM	Engineering Safety Management
LED	Light Emitting Diode
SIL	Safety Integrity Level

8.2 Specialized terms

hazard	A condition that could lead to an accident. A potential source of harm. A hazard should be referred to a system or product definition.
hazard log	The name used by CTA for a register of hazards.
risk	Combination of the likelihood of occurrence of harm and the severity of that harm.
risk estimation	The process of producing a measure of the level of risk being analyzed.
risk evaluation	The process of deciding whether the risk associated with a change to the railway is able.

9 Referenced Documents

This section provides full references to the documents referred to in the body of this volume.

[CSM-RA] Commission Regulation (EC) No 352/2009 of 24 April 2009 on the adoption of a Common Safety Method on Risk Evaluation and Acceptance

[50121-3-2] EN 50121-3-2 : 2006, 'Rolling stock – Apparatus'

[50126] EN 50126-1 : 1999, 'Railway applications —The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 1: Basic requirements and generic process'

[50129] EN 50126 : 2003, 'Railway applications —Communication, signalling and processing systems —Safety related electronic systems for signalling'

International Engineering Safety Management

Good Practice Handbook
Application Note 5

Published on behalf of the International Railway Industry
by Technical Programme Delivery Ltd