Preliminary Hazard and Risk Estimation Process for Introduction of New Level Crossing Technologies

Forward

The CRC for Rail Innovation was a collaborative effort with a mandate to conduct research on behalf of the Rail Industry. Utilising the capabilities of Universities, Industry and world leading researchers, nearly 140 research projects were undertaken. This report is an outcome of a research project which commenced under the guidance of the CRC for Rail Innovation.

As the CRC for Rail Innovation moved towards the end of its funding commitments, it looked for other ways to ensure the research was continued and outcomes continued to be available for Industry; a way to leave a Legacy for the Rail Industry. The result of this search was the creation of the Australasian Centre for Rail Innovation (ACRI).

While ACRI has created a research program which is independent of the work of the CRC for Rail Innovation, ACRI also has oversight and responsibility for continuing the activities of the CRC Legacy work. ACRI is pleased to be able to have continued, and finished, this important research project on behalf of the CRC for Rail Innovation.

ACRI is also pleased to be able to make a copy of this report available to you.
Important Notice and Disclaimer
This document is provided as a guide only. Following this preliminary hazard and risk analysis process does not in itself ensure safety, nor does it abrogate the responsibility of railway infrastructure managers to provide safety arguments and evidence for any proposed changes.

Authors
- Christian Wullems, CRC for Rail Innovation & Queensland University of Technology
- Anjum Naweed, CRC for Rail Innovation & CQUniversity Appleton Institute

Acknowledgements
This document has been written with support from the following people:
- Raden Kusumo, Office of the National Rail Safety Regulator
- Michael Lane, Office of the National Rail Safety Regulator
- Steve Bickley, Office of the National Rail Safety Regulator

Project Participants
- Queensland Rail
- Australian Rail Track Corporation
- V/Line
- Victrack
- RioTinto
- Railway Industry Safety & Standards Board
- Australasian Railways Association
- Public Transport Victoria
- Department of Transport and Main Roads, Queensland
- Department of Planning, Transport and Infrastructure, South Australia
- Queensland University of Technology
- Central Queensland University

Copyright
Copyright © 2015 CRC Rail IP Ltd.
This work is copyright. Apart from any use permitted under the Copyright Act 1968, no part may be reproduced by any process, nor may any other exclusive right be exercised, without the permission of the Australasian Centre for Rail Innovation.
Preliminary Hazard and Risk Estimation Process for Introduction of New Level Crossing Technologies

Document Control

Identification

<table>
<thead>
<tr>
<th>Document title</th>
<th>Number</th>
<th>Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preliminary Hazard Assessment Process for Introduction of New Level Crossing Technologies</td>
<td>1</td>
<td>0</td>
<td>28/07/2015</td>
</tr>
</tbody>
</table>

Document History

<table>
<thead>
<tr>
<th>Publication version</th>
<th>Effective date</th>
<th>Page(s) affected</th>
<th>Reason for and extent of change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>First draft</td>
<td>09/09/2014</td>
<td>All</td>
<td>New document</td>
</tr>
<tr>
<td>Second draft</td>
<td>19/12/2014</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Third draft</td>
<td>11/05/2015</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>Stakeholder review</td>
<td>17/06/2015</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>Final</td>
<td>28/07/2015</td>
<td>6, 22</td>
<td>Minor corrections</td>
</tr>
</tbody>
</table>

Authoring, Consultation and Approval

<table>
<thead>
<tr>
<th>Development stage</th>
<th>Who</th>
<th>When</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preliminary</td>
<td>CRC for Rail Innovation</td>
<td>09/09/2014</td>
</tr>
<tr>
<td>Final</td>
<td>CRC for Rail Innovation</td>
<td>28/07/2015</td>
</tr>
</tbody>
</table>
## Acronyms and Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARO</td>
<td>Accredited Rail Operator</td>
</tr>
<tr>
<td>CRC</td>
<td>Cooperative Research Centre</td>
</tr>
<tr>
<td>ETA</td>
<td>Event Tree Analysis</td>
</tr>
<tr>
<td>FTA</td>
<td>Fault Tree Analysis</td>
</tr>
<tr>
<td>HR</td>
<td>Hazard Rate</td>
</tr>
<tr>
<td>IRF</td>
<td>Individual Risk of Fatality</td>
</tr>
<tr>
<td>LX</td>
<td>Level Crossing</td>
</tr>
<tr>
<td>OEM</td>
<td>Original Equipment Manufacturer</td>
</tr>
<tr>
<td>ONRSR</td>
<td>Office of the National Rail Safety Regulator</td>
</tr>
<tr>
<td>OREDA</td>
<td>Offshore Reliability Data</td>
</tr>
<tr>
<td>PHA</td>
<td>Preliminary Hazard Analysis</td>
</tr>
<tr>
<td>PSSA</td>
<td>Preliminary System Safety Assessment</td>
</tr>
<tr>
<td>RIM</td>
<td>Rail Infrastructure Manager</td>
</tr>
<tr>
<td>RTO</td>
<td>Rail Transport Operators</td>
</tr>
<tr>
<td>SFAIRP</td>
<td>So Far As Is Reasonably Practicable</td>
</tr>
<tr>
<td>SIL</td>
<td>Safety Integrity Level</td>
</tr>
<tr>
<td>SRACs</td>
<td>Safety Related Application Conditions</td>
</tr>
<tr>
<td>THR</td>
<td>Tolerable Hazard Rate</td>
</tr>
</tbody>
</table>
Table Contents

1 Introduction ........................................................................................................................................7
   1.2 How This Document should be used .........................................................................................7
   1.3 Applicability of this Document .................................................................................................7

2 Part 1 - Process Overview .............................................................................................................9

3 Identifying Hazards ..........................................................................................................................12
   3.2 System definition and application conditions ..........................................................................13
   3.3 Defining level crossing subsystems and functions ..................................................................13
   3.4 Identifying causes of hazards ....................................................................................................13
   3.5 Analysing Consequences of Hazards .......................................................................................14

4 Risk Analysis – Comparing with a Reference System ......................................................................15
   4.2 Selection of a Reference System ...............................................................................................15
   4.3 System Safety Function Availability Analysis ...........................................................................16
   4.4 Estimating Hazard Rates ...........................................................................................................17
   4.5 Estimating Individual Risk of Fatality .......................................................................................18
   4.6 Comparison of Proposed System and Reference System IRFs ...............................................19

5 Evaluating Risk ..................................................................................................................................20
   5.1 Acceptability of Proposed System IRF ......................................................................................20
   5.2 Verifying IRF of Proposed System Meets Risk Acceptance Criteria .......................................20
   5.3 Development of a SFAIRP argument ..........................................................................................21

6 Human Factors ..................................................................................................................................22

7 Part 2 – Case Study ..........................................................................................................................23
   7.2 Case Study Scenario ....................................................................................................................23
   7.3 Identifying causes of hazards .....................................................................................................26
   7.4 Estimation of individual risk ......................................................................................................32

8 References .........................................................................................................................................34
1 Introduction

1.1.1 The Cooperative Research Centre for Rail Innovation’s low-cost level crossing risk and legal evaluation project (R2.121) has been tasked with the development of an argument to support the adoption of level crossing warning devices based on new or alternative technologies. An example includes devices that utilise innovative and alternative technologies such as wireless communications, alternative methods of train detection, and solar power in order to reduce lifecycle costs associated with construction, installation, commissioning, operation and maintenance.

1.2 How This Document should be used

1.2.1 It is expected that railway infrastructure managers (RIMs) can use this process at an early stage of a level crossing upgrade project to conduct a preliminary hazard analysis and determine the applicability of a proposed solution(s) at a specific level crossing site.

1.2.2 This document is provided in two parts: the first part describing a process for determining applicability of new level crossing technologies in a level crossing upgrade project; and the second part providing a case study with a worked example.

1.2.3 It should be emphasised that the described process does not in any way undermine or shortcut existing regulatory processes. Level crossing risk continues to be owned by the RIMs and is their responsibility.

1.3 Applicability of this Document

1.3.1 Suppliers of level crossing warning devices are generally required to provide a generic product safety case as part of a railway’s approval process; however, determining the applicability of a product for a specific level crossing site is frequently complicated by the inability to derive reliable safety targets. Statistical uncertainty due to sparseness of level crossing safety data is a large contributor to reliability issues of quantitative risk analysis. This often results in over-specification of safety requirements and potential rejection of technology candidates on the basis that they do not meet the highest safety requirements.

1.3.2 The application of European CENELEC norms (European Committee for Electrotechnical Standardization, 1999, 2003, 2006, 2007, 2011) is now commonplace for suppliers of railway safety equipment, particularly equipment comprised of electrical and electronic programmable logic devices. Safety Integrity Levels (SILs) relate to how often a safety-related system can enter into an unsafe state that can lead to system-level hazards, such that the hazard rate does not exceed tolerable hazard rate (THR) defined for a given hazard. The processes associated with developing systems to a given safety integrity level (SIL) provides assurance that the risk of systematic failure has been reduced to a level that meets a target tolerable hazard rate (THR).
1.3.1.3 THRs for each hazard related to a system are typically identified and assessed by a railway during the risk analysis phase of a project. SILs are intended to be used by railways to ensure a level crossing product can meet and fulfil the required THRs stipulated in an application safety case (European Committee for Electrotechnical Standardization, 2003). In the absence of defined targets (THRs), the proposed process provides an alternative methodology to determine the applicability of level crossing technology based on the performance of existing technology; ensuring the new technology is at least as safe as an equivalent reference type-approved system that would be applicable for installation at a specific site.

1.3.1.4 This process is expected to give the rail safety regulator confidence that a rigorous process was adopted in the preliminary analysis to support the safe application of new technologies at level crossings.
2 Part 1 - Process Overview

2.1.1.1 The process described in this document includes preliminary activities required to determine the applicability of a proposed solution before commencement of detailed site-specific design activities. The process is described in the context of the generic engineering safety management process described in the International Rail Industry’s Engineering Safety Management Handbook (Technical Programme Delivery Ltd., 2013a, 2013c). Figure 1 illustrates the scope of this document.

Figure 1. Generic engineering safety management process – Source: IESM (Technical Programme Delivery Ltd., 2013c)
2.1.1.2 This document focuses on the preliminary hazard and risk assessment process (Figure 3), which is comprised of the following phases:

- **Identifying hazards**: This phase involves identifying the hazard causes and analysing the consequences of the identified hazards;

- **Comparing with a reference system**: This phase involves comparing the proposed system with the reference system, using the analyses from the previous phase and an analysis of hazard rates to estimate the individual risk of fatality (IRF). The IRF is used to determine the safety of the proposed system with respect to the reference system from an individual risk perspective; and

- **Evaluating risk**: This phase involves evaluating the results of the previous phases and determining whether the IRF of the proposed system is acceptable, and developing a SFAIRP argument for the proposed system.

2.1.1.3 Each phase of the preliminary hazard and risk assessment process is discussed in the following sections.
Figure 2. Preliminary hazard and risk analysis process
3 Identifying Hazards

3.1.1 This section describes the process for identifying hazards of a generic level crossing warning system. Preliminary hazard analysis is performed at a sub-system level in order to facilitate a comparison of subsystems based on different technologies that implement level crossing functions. A multi-disciplinary team should perform this process and ideally include human factors specialists in addition to engineers.

3.1.2 A suitable analytical process is needed to determine generic failure modes at a functional level, and these can then be recorded into the hazard log to form the basis of the preliminary hazard and risk estimation process. The identified hazards are used to facilitate a comparison of different technologies (constituent subsystems) that implement the level crossing functions.

3.1.3 As an example, consider two type F level crossing warning systems (e.g. flashing lights only), where the only difference is the train detection subsystem. Train detection in one level crossing warning systems is implemented using track-circuits, whereas the other is implemented using axle-counting technology.

3.1.4 These level crossing warning systems can be compared at a subsystem level. By comparing hazard rates for hazards caused by failures of functions implemented by the train detection subsystem and any other subsystems affected by the change, it is possible to determine whether the change of technology will result in a net change of risk. However, it is vital for human factors to be considered for any changes of technology. This includes design and maintenance issues when the system is inactive, as well as any instances where the system interfaces with people in operating conditions when it is active (e.g. road user and pedestrian interfaces, interfaces to train driver, network control officers).

3.1.5 Functional failure analysis (FFA) can be used to determine generic failure modes at a functional level, the impact of the failure modes on the level crossing warning device, and the impact of the failure on the broader level crossing system (i.e. socio-technical system involving both road and rail systems).

3.1.6 This is a functional hazard assessment technique used to determine which functions of the system contribute to hazards and explore the effects of subsystem failures on other dependent subsystems and system-wide impact. With this method, hazardous failure modes can then be recorded in the hazard log to obtain a complete set of hazards.
3.2 System definition and application conditions

3.2.1.1 Before commencing preliminary hazard and risk assessment activities, the level crossing system including system boundaries and application conditions needs to be defined. This includes the following elements (European Committee for Electrotechnical Standardization, 1999):

- System Mission Profile – including type of rolling stock, wheel profiles, speed of rail traffic, volume of rail and road traffic, etc.;
- System Description;
- Operation and Maintenance Strategies;
- Operating Conditions – including environmental conditions (e.g. salinity, dust, temperature extremes, precipitation, etc.);
- Maintenance Conditions;
- Influence of Existing Infrastructure Constraints; and
- System boundaries - interfaces with the physical environment, other technological systems, humans, other railway and road authorities.

3.3 Defining level crossing subsystems and functions

3.3.1.1 Based on the system definition and application conditions, a generic level crossing is specified in terms of subsystems and functions those subsystems must provide. These functions will form the basis of the functional failure analysis (FFA) that will be used to facilitate comparison in the risk analysis phase.

3.4 Identifying causes of hazards

3.4.1.1 As discussed earlier in this section, functional failure analysis (FFA) is used to identify hazardous high-level failure modes that can potentially lead to injury or fatality. The FFA process involves defining the purpose and behaviour of each function, followed by an analysis where hypothetical failure modes are considered for each function and effects of the failure modes are determined. The results of this analysis are used to produce FFA tables, where failure modes with hazardous global / system impacts are added to the hazard log.

3.4.1.2 An example of hypothetical failure modes includes:

- Loss of function;
- Function provided when not required; and
- Incorrect operation of function.
3.5 Analysing Consequences of Hazards

3.5.1.1 A consequence analysis is performed for all identified hazards, quantifying the probability of a set of outcomes (e.g. collision, near-miss, non-event) for each hazard.

3.5.1.2 Site-specific application conditions (defined in the system definition phase) need to be taken into consideration when determining the range of possible consequences and quantifying them with probabilities. For example, the probability of a collision between a train and road vehicle will be sensitive to road and rail traffic volumes at the level crossing site.

3.5.1.3 Event tree analysis (ETA) has been used in the example to model consequences of hazard H1. ETA starts with an initiating event (i.e. the hazard). Accident scenarios resulting from the initiating event need to be identified and a logic tree is built by identifying intermediate events, in which actions, decisions or potential failure of protective mechanisms can result in escalation or control / containment of a given accident scenario.

3.5.1.4 Failure probabilities are assigned to intermediate events and can be quantified using a number of methods including statistical analysis, failure analysis (e.g. fault-tree analysis of the probability of failure of a protective mechanism), and expert judgement.
4 Risk Analysis – Comparing with a Reference System

4.1.1 This section describes the risk analysis process, comparing the proposed system with a reference system. The process involves three steps that need to be performed for both the reference and proposed systems (refer to Figure 2):

- Perform a system safety function availability analysis (SSFAA);
- For each hazard, estimate hazard rates for component failures that result in loss of safety function; and
- Estimate individual risk of fatality (IRF) including complete set of hazards and consequences.

4.1.2 The risk of the proposed system is then evaluated by comparing the IRF of both systems against an agreed acceptance criteria. The following subsections describe the process in more detail.

4.2 Selection of a Reference System

4.2.1 Using the site-specific application conditions (defined in the system definition phase), an appropriate reference system must be selected based on current accepted practice. For example, for a relatively low-exposure non-urban level crossing site with duplicated bi-directional track, current practice may require consideration of an automatic type F level crossing with half-booms, controlled by two approach track circuits, two control track circuits and an island track circuit (or potentially a grade predictor in non-electrified territory).

4.2.2 For a low-exposure occupational crossing, current practice may require consideration of a type F level crossing with flashing lights only.

4.2.3 It is expected that the reference system:

- Would reduce risk to a level that meets risk acceptance criteria for the specific site;
- Would meet SFAIRP requirement at the specific site; and
- Is type approved.
4.3 System Safety Function Availability Analysis

4.3.1 A system safety function availability analysis (SSFAA) needs to be conducted for both reference and proposed systems. This analysis requires examining failure modes that can affect the availability of the safety function for each subsystem.

4.3.1.2 Hazards identified from the functional failure analysis relate to failure modes that affect safety-related functions implemented by subsystems of the level crossing warning system (e.g. train detection function provided by the train detection subsystem). These hazardous failure modes affect the availability of the system safety function (i.e. provide sufficient warning to road users of an approaching train).

4.3.1.3 In order to estimate hazard rates, one approach involves using fault-trees constructed for each hazard, comprised of the failure modes of subsystems that cause the hazard using the output from the hazard identification phase. These fault trees are developed to a level where component failures for subsystems implementing constituent safety functions can be quantified, thus providing hazard rates.

4.3.1.4 For simplicity, consider a proposed type F level crossing warning system with half-booms where the power supply subsystem of the reference system design is replaced with a solar power supply system. The effect of changing the subsystem from the reference technology to the new / alternative technology needs to be considered for each identified hazard and how the change of subsystem can affect dependent subsystems and their constituent safety functions.

4.3.1.5 An example of the hazard “no road signal for approaching train” is illustrated in Figure 3 for the change of power supply subsystem. A change in the rate of failure of the power supply system directly impacts the hazard rate due to dependencies in the road signalling subsystem. For example, the train detection subsystem has a fail-safe design for which loss of power causes the train detection subsystem to fail to an occupied state. It is the loss of power to the road signalling subsystem that directly results in the hazard.
4.4 Estimating Hazard Rates

4.4.1.1 A recommended method for estimation of hazard rates is Fault tree analysis (FTA).

4.4.1.2 FTA is a deductive failure analysis technique that can be used to quantify hazard rates. Fault trees for each hazard can be constructed from the SSFAA phase of the proposed process, and quantified by obtaining failure data for component failures of each subsystem.

4.4.1.3 Fault trees use Boolean logic to combine a series of subsystem failure events, facilitating the quantification of hazard rate for each hazard. These hazard rates will be used in the estimation of individual risk.

4.4.1.4 Failure data to quantify component failures can potentially be sourced from the following places:

- For reference systems, existing level crossing component-level failure data could be obtained directly from RIMs
- For proposed systems, failure data would be provided by suppliers / other railways
- Where failure data is not available, component failure data could be sourced from databases (e.g. MIL-HDBK-217, OREDA, etc.)
4.5 Estimating Individual Risk of Fatality

4.5.1.1 Individual risk of fatality has been chosen as a measure of risk for comparison of the reference and proposed systems, as it errs on the side of safety. For example, if an occupational level crossing is assessed, even though relatively small volumes of road traffic might utilise the crossing, a farmer using the crossing several times a day would have a higher exposure to the risk than calculations that consider collective risk.

4.5.1.2 Individual risk calculations in this process are used to consider the worst-case exposure an individual for the determination of whether the proposed system is at least as safe as the reference. The suggested formula for calculating individual risk is detailed below.

4.5.1.3 The equation for determination of individual risk is given below (European Committee for Electrotechnical Standardization, 2010):

\[ IRF_i = \sum_{all \ hazards \ H_j} N_i \left( HR_j \times (D_j + E_{ij}) \sum_{accidents \ A_k} C_j^k \times F_i^k \right) \]

Where \( IRF_i \) is the individual risk of fatality, \( N_i \) is the number of uses, \( HR_j \) is the hazard rate for hazard \( j \), \( D_j \) is the duration of hazard \( j \), \( E_{ij} \) is the exposure of individual \( i \) to hazard \( j \), \( C_j^k \) is the consequence probability for hazard \( j \) leading to accident \( k \), and \( F_i^k \) is the probability of fatality for individual \( i \) in accident type \( k \).

4.5.1.4 Another interpretation of the above formula is detailed below, which considers the probability that hazard \( j \) already exists and the probability that individual \( i \) is exposed to hazard \( j \) (European Committee for Electrotechnical Standardization, 2010):

\[ IRF_i = \sum_{all \ hazards \ H_j} \left( \left[ N_i \times (HR_j \times D_j) + HR_j \times (N_i \times E_{ij}) \right] \sum_{accidents \ A_k} C_j^k \times F_i^k \right) \]
4.5.1.5 In calculating the IRF of the reference system and proposed system the following needs to be considered:

- Accident types (e.g. collision between road vehicle and train, boom strike, etc.);
- Target group of the individual (e.g. general public (road users, pedestrians), passengers and employees);
- Hazard rates for all identified hazards (output from hazard estimation);
- Duration of the hazard and probability that the hazardous state already existed;
- Estimated exposure of an individual to the hazard from the target group (informed by site-specific application conditions from the system definition);
- Consequence probability from event-tree analysis (output from the analysis of consequences); and
- Probability of fatality for an individual in given accident type, sourced from level crossing accident statistics.

4.6 Comparison of Proposed System and Reference System IRFs

4.6.1.1 The comparison of individual risk of fatality (IRF) facilitates the appraisal of system risk, whilst providing some flexibility for changes to failure rates in different subsystems in order to achieve at least the same level of safety as the reference system.

4.6.1.2 Once the IRF has been calculated for target groups for both reference and proposed systems, the values are compared against acceptance criteria.
5 Evaluating Risk

5.1 Acceptability of Proposed System IRF

5.1.1 Preliminary acceptability of a proposed system is determined by a comparison of IRF values from the proposed and reference systems and whether acceptance criteria are met. It is assumed that the reference system is based on current good practice and already satisfies the SFAIRP requirement.

5.1.1.2 If the IRF of the proposed system is less than or equivalent to the reference system, a SFAIRP argument can be developed on the basis of the cost of other options and further risk reduction being grossly disproportionate to the benefit.

5.1.1.3 If the IRF of the proposed system is greater than the reference system, further analysis is required to determine applicability. This includes:

- Demonstration that the proposed system would reduce risk to a level that meets the risk acceptance criteria for the specific site;
- Demonstration that the cost of other options to reduce risk reduction is grossly disproportionate to the benefit; and
- Demonstration that the cost of further risk reduction in the proposed system to at least meet the IRF of the reference system is grossly disproportionate to the benefit.

5.1.1.4 In some circumstances, there may be a compelling case for the installation of a warning system with a higher IRF at a low-exposure site (e.g. occupational and farm crossings) given that the cost of installing a system with an equivalent or better IRF may be excessive.

5.2 Verifying IRF of Proposed System Meets Risk Acceptance Criteria

5.2.1 The IRF of the proposed system must meet the risk acceptance criteria defined in the railway’s safety management system, providing evidence that the risk is tolerable. If this risk is not tolerable, then the proposed system is not suitable.
5.3 Development of a SFAIRP argument

5.3.1.1 The development of a SFAIRP argument is outside the scope of this document. Refer to the Meaning of Duty to Ensure Safety So Far As Is Reasonably Practicable Guideline (Office of the National Rail Safety Regulator, 2014) for more information.

5.3.1.2 To avoid confusion, it should be noted that the SFAIRP argument should be based on the estimation of collective risk at a specific level crossing site, not individual risk, consistent with guidance in RSSB Taking Safe Decisions v2.

5.3.1.3 The proposed process uses the individual risk of fatality (IRF) to compare the safety of the proposed system with the reference system, as it errs on the side of safety. The IRF is not used in making a SFAIRP argument. The IRF can be used as the basis to form a SFAIRP argument; however, this SFAIRP argument is not complete and further analysis is required to determine the SFAIRP position. Refer to the ONRSR SFAIRP guideline for formulating the SFAIRP argument (Office of the National Rail Safety Regulator, 2014).
6 Human Factors

6.1.1.1 Human factors are concerned with applying what is known about people, their abilities, characteristics and limitations to the design of the equipment they use, the environments in which they function, and the jobs they perform.

6.1.1.2 As rail level crossings are designed to control the flow of traffic in highly dynamic situations, human factors must be considered in the way that the level crossing technologies and systems are interacted with by the user (e.g. road-user, pedestrian, train driver, network control officer), as well as the way that people engage with them over their life-cycle (e.g. designers, maintainers). For this reason, human factors are vital when considering the applicability of new technologies for rail level crossings.

6.1.1.3 Level crossings are fundamentally complex and dynamic socio-technical systems, where degraded modes of operation involve numerous procedures. It is important to recognise that any changes to a system should be accompanied by due consideration of changes to existing procedures or processes. It is also important to recognise that even if the technology is technically safe, failures may still encourage risk-taking behaviours or interactions that create unsafe situations.

6.1.1.4 For this reason, it is useful to assess the human contribution to risk with techniques that assess human reliability and quantify human error. Such tools already exist based on calculating the contribution of risk for humans that work within rail (e.g. the Railway Action Reliability Assessment Tool, RSSB) but similar techniques may be used to assess the risk for others (e.g. road users).
7 Part 2 – Case Study

7.1.1 A simple case study has been provided to demonstrate the principles described in part 1 for an infrastructure manager that is upgrading a level crossing with passive controls. The infrastructure manager has several upgrade options available including a standard type F level crossing warning system with mains power and a proposed system, identical to the standard type F level crossing warning system, except solar powered. This case study illustrates the evaluation of a proposed system, considering the impact of replacing the standard type F level crossing warning system mains power supply with a solar power supply. The case study focuses on the following aspects of the process:

- Hazardous events that are caused by power supply failures;
- Simplified fault-trees to demonstrate how power supply failures can lead to the top events. The fault-tree analysis assumes that there are no changes in the batteries and other level crossing subsystems;
- Calculation of the individual risk of fatality (IRF) based on the failure rates of a council power supply and solar power supply; and
- Comparison of both IRFs to provide evidence that the proposed level crossing warning system is at least as safe as a standard type F level crossing warning system in terms of individual risk.

7.1.2 It is expected that the analyses would be used to support a SFAIRP argument, which includes a comparison of costs and benefits of the proposed system compared with the standard type F level crossing warning system. The development of a SFAIRP argument is outside the scope of this case study. Refer to the SFAIRP guideline (Office of the National Rail Safety Regulator, 2014) for more information.

7.1.3 Human factors issues have not been evaluated in this case study due to the difficulty of performing such analyses for a high-level hypothetical scenario. This does not mean human factors are not relevant to this scenario.

7.2 Case Study Scenario

7.2.1 For simplicity, the case study assumes a standard type F level crossing warning system (flashing lights only) is to be installed at a level crossing with a single bi-directional track.

7.2.2 The following assumptions are made for a standard type F level crossing in this case study:

- The level crossing warning system is an automatic warning system but is autonomous too in that it is not associated with an interlocking, ERTMS object controller, etc.
- The warning system is activated and deactivated by track circuits on the level crossing approaches and island;
• The warning system includes a monitoring system that raises alarms in the operations centre for power supply fault conditions including loss of mains supply, low battery, charging failure, etc. The monitoring system sends a periodic heartbeat (e.g. every minute), such that immediate failure of power supply is detected in the test interval;

• The warning system does not provide healthy state indication to rail traffic. It is assumed trains have right of way unless informed of a level crossing failure by a network control officer;

• The batteries are of sufficient capacity to operate the level crossing warning system, associated control equipment, train detection equipment and any railway signalling fed from the level crossing location for a minimum period of 48 hours with 10% residual capacity under average rail traffic densities;

• The mains power supply is derived from the supply authority, and batteries are sized to meet capacity requirements; and

• The solar power supply’s solar panels and batteries are sized to meet the capacity requirements for the specific location (taking into consideration weather, solar yield, etc.).

7.2.1.3 A standard type F level crossing is illustrated in Figure 4.

Figure 4. Reference level crossing

Figure 5. Proposed change to reference level crossing system
7.2.1.4 The following assumptions are for procedures that are executed when a fault is detected in the power supply subsystem:

- When a level crossing monitoring system raises an alarm in the operations centre indicating a fault in the power supply subsystem (e.g. failure of a charger), it is assumed that arrangements will be made for a Signals Maintenance representative to attend the site within a period that is well within the 48-hour operating capacity of the batteries. It is additionally assumed that the network control officer will warn rail traffic crews about the potentially faulty warning equipment;

- In the case of an immediate failure of the power supply subsystem, it is assumed that the network control officer will warn rail traffic crews that the warning equipment is faulty. The network control officer is additionally required to arrange for the crossing to be protected by emergency services or road traffic controllers, or arrange for the crossing to be closed to road and pedestrian traffic. In the case of an immediate failure of the power supply subsystem, it is also assumed that arrangements will also be made for a signals maintenance representative to attend the site;

- A conservative assumption is made on the duration of the hazard in the case of an immediate failure of the power supply subsystem. A duration of 1 hour is assumed from the time of the failure to the time the failure is isolated (i.e. to when the level crossing is protected).

- The reliability of procedures for protecting the crossing in the case of a fault or failure in the power supply subsystem have not been considered in this case study, as procedures are not expected to change with the change from mains to solar power supply. Where changes with respect to the reference system result in procedural changes, the reliability of procedures must be taken into consideration from a human performance and human reliability assessment perspective.

7.2.1.5 The following table illustrates a set of subsystems and functions those subsystems provide for this level crossing type.

<table>
<thead>
<tr>
<th>Subsystems</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Train detection subsystem</td>
<td>• Detect train has passed strike-in point on LX approach&lt;br&gt;• Detect train has cleared LX island</td>
</tr>
<tr>
<td>Level crossing warning control subsystem</td>
<td>• Activate road signals when train passes strike-in point&lt;br&gt;• Deactivate road signals when train has cleared LX island&lt;br&gt;• Provide continuous operation of road signals active from strike-in to clearance of LX island&lt;br&gt;• Activate road signals when failure state detected</td>
</tr>
<tr>
<td>Road signalling subsystem (including audible warning)</td>
<td>• Flash RX5 lamps in alternating pattern&lt;br&gt;• Sound audible warning</td>
</tr>
<tr>
<td>Remote monitoring and diagnostic subsystem</td>
<td>• Raise fault alarm&lt;br&gt;• Detect faults in road signalling subsystem&lt;br&gt;• Detect faults in train detection subsystem&lt;br&gt;• Detect faults in power supply subsystem</td>
</tr>
</tbody>
</table>
Power supply subsystem • Provide power to subsystems
Connectivity subsystem • Provide connectivity between subsystems (i.e. cables)

7.3 Identifying causes of hazards

7.3.1.1 A functional failure analysis (FFA) is performed for the identified level crossing subsystems and functions. Three hypothetical failure modes are considered for each function:

- Loss of function;
- Function provided when not required; and
- Incorrect operation of function.

7.3.1.2 The FFA table below illustrates the output of an FFA specific to the power supply subsystem.

Table 2. Functional failure analysis - Power supply subsystem

<table>
<thead>
<tr>
<th>ID</th>
<th>Subsystem</th>
<th>Function</th>
<th>Failure Mode</th>
<th>Applicable</th>
<th>Failure Description</th>
<th>Local Impact</th>
<th>Global/System Impact</th>
<th>Hazardous</th>
</tr>
</thead>
<tbody>
<tr>
<td>FFA-5.1.1</td>
<td>Power supply subsystem</td>
<td>Supply power to train detection subsystem</td>
<td>Loss of function</td>
<td>Y</td>
<td>Failure to provide power to train detection subsystem</td>
<td>Failure results in a track occupancy state of occupied for affected track circuits.</td>
<td>Road signals (LX failure mode) are activated and remote monitoring and diagnostic subsystem raises an alarm.</td>
<td>N*</td>
</tr>
<tr>
<td></td>
<td>Power supply subsystem</td>
<td>Supply power to train detection subsystem</td>
<td>Function provided when not required</td>
<td>NA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FFA-5.1.2</td>
<td>Power supply subsystem</td>
<td>Supply power to train detection subsystem</td>
<td>Incorrect operation of function</td>
<td>Y</td>
<td>Power supplied to train detection subsystem is outside of design limits</td>
<td>Failure might result in blown fuse(s), causing loss of power to the train detection subsystem. (See FFA-5.1.1)</td>
<td>Road signals (LX failure mode) are activated and remote monitoring and diagnostic subsystem raises an alarm.</td>
<td>N*</td>
</tr>
<tr>
<td>FFA-5.1.3</td>
<td>Power supply subsystem</td>
<td>Supply power to road signalling subsystem</td>
<td>Loss of function</td>
<td>Y</td>
<td>Failure to provide power to road signalling subsystem</td>
<td>Failure results in road signals not operating on approach of a train.</td>
<td>Remote monitoring and diagnostic subsystem raises an alarm. Entry and traversal of a train at an unprotected LX may result in a collision between road vehicle(s) and train, resulting in potential injuries and/or fatalities</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>Power supply subsystem</td>
<td>Supply power to road signalling subsystem</td>
<td>Function provided when not required</td>
<td>NA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Subsystem</td>
<td>Function</td>
<td>Failure Mode</td>
<td>Applicable</td>
<td>Failure Description</td>
<td>Local Impact</td>
<td>Global/System Impact</td>
<td>Hazardous</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------</td>
<td>----------------------</td>
<td>-----------------------------------</td>
<td>------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>FFA- 5.1.4</td>
<td>Power supply subsystem</td>
<td>Detect faults in road signalling subsystem</td>
<td>Incorrect operation of function</td>
<td>Y</td>
<td>Power supplied to road signalling subsystem is outside of design limits</td>
<td>Failure might result in blown fuse(s), causing loss of power to the road signalling. (See FFA-5.1.1)</td>
<td>Remote monitoring and diagnostic subsystem raises an alarm. Entry and traversal of a train at an unprotected LX may result in a collision between road vehicle(s) and train, resulting in potential injuries and/or fatalities</td>
<td>Y</td>
</tr>
</tbody>
</table>

*Not hazardous only when road users interact with the level crossing as intended during the right-side failure duration (time from initiation of failure condition to isolation) and that the assumed procedures are executed as intended.

7.3.1.3 Failure modes in the FFA that result in common hazards are grouped as single hazards with a combined set of causal failure modes. This is illustrated in the example below.

Table 3. Failure modes leading to common hazards

<table>
<thead>
<tr>
<th>Top-level Hazards</th>
<th>Causal Failure Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1</td>
<td></td>
</tr>
<tr>
<td>No road signal for approaching train</td>
<td>FFA-5.1.3 Failure to provide power to road signalling subsystem</td>
</tr>
<tr>
<td></td>
<td>FFA-5.1.4 Power supplied to road signalling subsystem is outside of design limits</td>
</tr>
</tbody>
</table>

7.3.1.4 As the change only affects the power supply subsystem (i.e. there are no changes in the batteries and other LX subsystems), the analysis focuses on hazardous events that are caused by power supply failures.

7.3.1.5 Fault-tree analysis has been used to quantify the hazard rate of H1 for the reference system and the proposed system (Figure 6 and Figure 7).
Figure 6. Fault-tree for power supply failures leading to hazard GT-FFA-5.1.3 / H1 (mains supply)
Figure 7. Fault-tree for power supply failures leading to GT-LPWR-PSS (solar supply)
7.3.1.6 The following tables detail the values used in the case study analyses and are provided for illustrative purposes only.

### Table 4. Accidents

<table>
<thead>
<tr>
<th>Accident ID</th>
<th>Accident</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Collision between rail vehicles and road vehicles at level crossings</td>
</tr>
<tr>
<td>A2</td>
<td>Collision between rail vehicles and persons (pedestrians or track workers) at level crossings</td>
</tr>
</tbody>
</table>

### Table 5. Fault-tree events

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
<th>Failure rate (per hour)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EV-BAT-CHG</td>
<td>Battery charger</td>
<td>1.127E-6</td>
</tr>
<tr>
<td>EV-BAT-FL</td>
<td>Battery</td>
<td>1.369E-2</td>
</tr>
<tr>
<td>EV-PF-DET</td>
<td>Failure to detect onset of power supply failure</td>
<td>1.539E-4</td>
</tr>
<tr>
<td>EV-MAINS-SPLY</td>
<td>Charging power supply failure (Mains)</td>
<td>5.708E-4</td>
</tr>
<tr>
<td>EV-SOLAR-SPLY</td>
<td>Charging power supply failure (Solar)</td>
<td>4.566E-6</td>
</tr>
</tbody>
</table>

### Table 6. Event-tree events

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
<th>No</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>EV-RU-A-BCF</td>
<td>Road user arrives before crossing fixed</td>
<td>0.001</td>
<td>0.999</td>
</tr>
<tr>
<td>EV-APPR-T-RU</td>
<td>Train approaching as road user traverses LX</td>
<td>0.878</td>
<td>0.122</td>
</tr>
<tr>
<td>EV-RU-AV-COL</td>
<td>Road user notices approaching train and is able to avoid collision</td>
<td>0.1</td>
<td>0.9</td>
</tr>
<tr>
<td>EV-TD-ASS</td>
<td>Train driver able to stop train short of road user</td>
<td>0.99</td>
<td>0.01</td>
</tr>
</tbody>
</table>
7.3.1.7 The event tree model used to quantify consequences probabilities for hazard H1 leading to accident A1 is illustrated in Figure 8.

![Event Tree](attachment:figure8.png)

**Figure 8. Event tree analysis (ETA) for H1**

7.3.1.8 A summary of consequence probabilities determined from the event tree analysis is provided in Table 7.

**Table 7. Summary of consequence probabilities for hazard H1 leading to accident A1**

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-event</td>
<td>8.777E-01</td>
</tr>
<tr>
<td>Near-miss</td>
<td>1.102E-01</td>
</tr>
<tr>
<td>Collision</td>
<td>1.210E-02</td>
</tr>
</tbody>
</table>
7.4 Estimation of individual risk

7.4.1.1 Individual risk is estimated using the following formula (European Committee for Electrotechnical Standardization, 2010):

\[
IRF_i = \sum_{\text{all hazards } H_j} N_i \left( HR_j \times (D_j + E_{ij}) \right) \sum_{\text{accidents } A_k} C_j^k \times F_i^k
\]

Where \( IRF_i \) is the individual risk of fatality, \( N_i \) is the number of uses, \( HR_j \) is the hazard rate for hazard \( j \), \( D_j \) is the duration of hazard \( j \), \( E_{ij} \) is the exposure of individual \( i \) to hazard \( j \), \( C_j^k \) is the consequence probability for hazard \( j \) leading to accident \( k \), and \( F_i^k \) is the probability of fatality for individual \( i \) in accident type \( k \).

7.4.1.2 For the purpose of the case study, one type of individual is considered: a regular road user of a level crossing. The worst case user is assumed to traverse the level crossing approximately 3000 times per year (approximately 8 times per day). Other uses such as pedestrians and cyclists are not considered in this case study.

7.4.1.3 Hazard H1 is assumed to last longer than the individual exposure time (the time required for the user to traverse the level crossing). Therefore, the individual exposure time \( E_{ij} \) can be disregarded and a conservative hazard duration time of 1 hour is considered. This is the time the LX remains in the hazardous state until negated (e.g. via procedures) or repaired.

Table 8. Parameters for IRF calculation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>( HR_{H1(RS)} )</td>
<td>Hazard rate for H1 (reference system)</td>
<td>2.107E-6</td>
</tr>
<tr>
<td>( HR_{H1(PS)} )</td>
<td>Hazard rate for H1 (proposed system)</td>
<td>2.020E-6</td>
</tr>
<tr>
<td>( D_{H1} )</td>
<td>Duration of hazard H1</td>
<td>1 hour</td>
</tr>
<tr>
<td>( C_{A1} )</td>
<td>Consequence probability for hazard H1 leading to accident A1</td>
<td>1.210E-02</td>
</tr>
<tr>
<td>( F_{i,A1} )</td>
<td>Probability of fatality for individual ( i ) in accident type ( A1 )</td>
<td>0.18</td>
</tr>
<tr>
<td>( N_i )</td>
<td>Number of uses of the LX for individual ( i )</td>
<td>3000 per year</td>
</tr>
</tbody>
</table>

7.4.1.4 Only Accident A1 has been considered in this case study.

7.4.1.5 Individual risk of fatality for hazard H1 (reference system) and for accident type A1:

\[
IRF_{i,H1(RS),A1} = N_i \left( (HR_{H1} \times D_{H1}) (C_{A1}^i \times F_{i,A1}^i) \right)
\]

\[
IRF_{i,H1(RS),A1} = 1.380 \times 10^{-5}
\]
7.4.1.6 Individual risk of fatality for hazard H1 (proposed system) and for accident type A1:

\[ IRF_{H1(PS),A1} = N_i \left( (HR_{H1} \times D_{H1})(C_{H1}^{A1} \times F_{i}^{A1}) \right) \]

\[ IRF_{H1(PS),A1} = 1.320 \times 10^{-5} \]

7.4.1.7 In this case study, the infrastructure manager would have based the upgrade argument on the safety improvement afforded by upgrading the protection at the site from passive to active controls.

7.4.1.8 Risk mitigation options considered by the infrastructure manager would have included various designs of active protection including a mains-powered standard type F level crossing warning system (flashing lights only) and the proposed solar powered option.

7.4.1.9 The solar powered option (proposed system) has demonstrated a marginally better risk reduction than the mains powered option (reference system); i.e. \( IRF_{H1(PS),A1} \) is less than the reference system \( IRF_{H1(RS),A1} \), and therefore could be considered to be at least as safe as the reference system. It is assumed that the reference system meets risk acceptance criteria at the site.

7.4.1.10 In the case that the proposed system IRF would have exceeded the reference system IRF, a demonstration that the residual risk at the specific site meets risk acceptance criteria after treatment with the proposed system would be needed. Furthermore, a SFAIRP argument would need to:

- Demonstrate that that the cost of other options and further risk reduction is grossly disproportionate to the benefit; and
- Justify that the cost of further risk reduction for the proposed system to at least meet the reference system IRF, would be grossly disproportionate to this magnitude of risk reduction.

A complete SFAIRP argument is required. Refer to ONRSR guidance for formulation of a complete argument (Office of the National Rail Safety Regulator, 2014).
8 References


