

Ref:	NR/L2/SIG/11201 – Mod A9
Issue:	4
Date:	04/06/2011
Compliance date:	03/09/2011

Level 2

Signalling Design: Module A9 - Safety System

Endorsement and Authorisation

For endorsement and authorisation, please refer to
NR/L2/SIG/11201

This document is the property of Network Rail. It shall not be reproduced in whole or part nor disclosed to a third party without the written permission of Network Rail.
© Copyright 2011 Network Rail.

Uncontrolled copy once printed from its electronic source.

Published and Issued by Network Rail, Kings Place, 90 York Way, London. N1 9AG.



Ref:	NR/L2/SIG/11201 – Mod A9
Issue:	4
Date:	04/06/2011
Compliance date:	03/09/2011

Issue record

Issue	Date	Comments
4	June 2011	Modularisation of handbook and guidance notes, contains content of former NR/GN/SIG/11701 Part R.

Compliance

This Module is mandatory and shall be complied with by Network Rail and its contractors if applicable from 03/09/2011.

When this standard is implemented, it is permissible for all projects that have formally completed GRIP Stage 3 (Option Selection) to continue to comply with the issue of any relevant Network Rail standards current when GRIP Stage 3 was completed and not to comply with requirements contained herein, unless stipulated otherwise in the scope of this standard.

Disclaimer

In issuing this document for its stated purpose, Network Rail makes no warranties, express or implied, that compliance with all or any documents it issues is sufficient on its own to confirm safe systems of work or operation. Users are reminded of their own duties under health and safety legislation.

Supply

Copies of documents are available electronically, within Network Rail's organisation. Hard copies of this document may be available to Network Rail people on request to the relevant controlled publication distributor. Other organisations may obtain copies of this document from IHS. Tel: 01344 328039.

Ref:	NR/L2/SIG/11201 – Mod A9
Issue:	4
Date:	04/06/2011
Compliance date:	03/09/2011

Contents

1 Introduction	4
2 Risk Assessment	4
2.1 Hazard Log	4
2.2 Causal Analysis	5
2.3 Consequence Analysis	6
2.4 Loss Analysis	8
2.5 Options and Impact Analysis	9
2.6 Compliance with Legal Duty	10
3 Documentation	12

Ref:	NR/L2/SIG/11201 – Mod A9
Issue:	4
Date:	04/06/2011
Compliance date:	03/09/2011

1 Introduction

Some type of risk assessment to demonstrate functional safety should be used whenever departure from a Network Rail company standard is proposed. The degree of detail in the analysis should reflect the degree of departure from the standard and the level of risk involved.

It should be demonstrated that any hazards identified present an acceptable risk to passengers, public or employees. Mitigation measures shall be implemented for those hazards which present an unacceptable risk.

Similar risk assessments may also be performed where it is desired to improve the reliability, availability, maintainability or safety of an existing system or element.

It is generally simpler to analyse the system at signalling function level (i.e. signals, points, level crossings, etc.), but, where justified by the risk, a safety analysis at component level (such as relays and contacts) may be appropriate.

2 Risk Assessment

An example of risk assessment is given in Figures 1 to 10, relating to automatic signal 103 on the layout provided in Figure 12. It should be noted that an actual risk assessment requires full calculations and reference to source information, which have not been given here for the sake of simplicity. All values quoted are illustrative only.

2.1 Hazard Log

A simple hazard log should be created using failure modes, effects and criticality analysis (FMECA), or similar techniques. Further information is given in [BS 5760: Part 5](#).

All hazards should be identified and logged. Creative methods of hazard identification, such as brainstorming, should be used for novel applications. The ranking obtained may be used to select the hazards that require further analysis. The range of values for frequency (F) and severity (S) should be individually defined, for example:

F=1	Less than 10 yearly	S=1	Minor injury
F=2	5 to 10 yearly	S=2	Major injury
F=3	1 to 5 yearly	S=3	Multiple major injuries
F=4	Monthly to yearly	S=4	Single fatality
F=5	Daily to monthly	S=5	Multiple fatalities

An example of a hazard log is shown in Figure 1. Wrong side failures (WSFs) have been identified in the figures, but note that right side failures also give rise to hazards and have, by definition, a great frequency.

Ref:	NR/L2/SIG/11201 – Mod A9
Issue:	4
Date:	04/06/2011
Compliance date:	03/09/2011

Ref. No.	Hazard Description	Estimated Frequency F	Estimated Severity S	Hazard Ranking F x S	Remarks
1	Train SPADs signal.	3	1	3	Possible WSF of distant signal (unlikely), isolation of AWS, poor visibility, or driver distraction. Likely to be low speed run-by. Protected by banner 105BR.
2	Signal off when train in section (WSF).	1	4	4	Possible WSF of a track section. Could result in collision with train in platform.
3	Signal comes off momentarily when train passes from EK to EL track (WSF).	3	1	3	Possible interface problem between transmission systems. Unlikely to occur at the same time as next train approaching (headway does not allow).
4	Signal not displaying red aspect when signaller's replacement controls on (WSF).	3	2	6	Possible WSF of transmission system. Could result in fatality of track worker(s).
5	Signal off when signal 105 ahead on and signal or banner lamp extinguished (WSF).	1	3	3	Possible WSF of signal circuit. Could result in a serious SPAD at signal 105.
6	Signal off when detection failed on 705 points in overlap (WSF).	2	1	2	Possible WSF of detection circuit. Could result in a derailment if the train SPADs signal 105.
7	Signal green when signal 105 ahead at red (WSF).	1	1	1	Minimal consequence, as braking distance available from 105BR banner to signal 105 ahead.
8	Unable to obtain proceed aspect.	4	1	4	Right side failure. Hazard from service disruption and instructing trains to pass signal at danger (or out).
9	Red lamp out when controls on.	3	1	3	Protected by signal in rear held at red, but hazard from trains proceeding at caution through long section from previous signal box.
10	Signal replaced in front of train.	3	1	3	Possible detection failure when 705 points swung in the overlap. Hazard from emergency braking.

Figure 1 – Hazard Log for Auto Signal No.103

2.2 Causal Analysis

Where necessary, a fault tree should be used to more accurately determine the probability of each hazard as an annual frequency. The symbols used should be defined on the drawing (see [BS 5760: Part 7](#)).

The probabilities of the basic events (shown numbered in the examples) may be obtained from such sources as:

- the train working timetable;
- component failure statistics (gathered in accordance with [GE/RT8106](#));
- failure modes for different types of component, listed in [BS EN 50129](#);
- historical operating experience of established systems.

The fault tree connects events by means of 'AND' gates and 'OR' gates. The probability of the top event may be obtained mathematically by summing the probabilities at OR gates and taking the product at AND gates.