



Engineering Safety Management

Yellow Book 3

Application Note 1 ***Railway-Level Issues***

Issue 1.0

Disclaimer

Railway Safety has taken trouble to make sure that this document is accurate and useful, but it is only a guide. The company does not give any form of guarantee that following the recommendations in this document will be enough to ensure safety. Railway Safety will not be liable to pay compensation to anyone who uses this guide.

Published by Railway Safety on behalf of the UK rail industry

Contents

1	Introduction	1
2	Specification Issues	2
2.1	The Problem	2
2.2	Guidance	2
3	Assumptions, Dependencies and Caveats	3
3.1	Introduction	3
3.2	Identifying ADCs that you will place on others	4
3.3	Identifying ADCs that others will place on you	4
3.4	Documenting ADCs	5
3.5	Resolving ADCs	6
4	Failure Detection and Modelling	8
4.1	Introduction	8
4.2	Failure detection	9
4.3	Modelling failure and its detection	9
4.4	Estimation of time at risk	10
5	Referenced documents	11
6	Acknowledgements	11
A	Appendix: Example Specification Topics	12

List of Figures

Figure 1 - Example Assumptions, Dependencies & Caveats	4
Figure 2 - Example State Transition Diagram	10

I INTRODUCTION

The Yellow Book Steering Group has decided to supplement Yellow Book 3 with a series of application notes. Each note provides more detailed guidance on a particular aspect of the Yellow Book. This document is an application note for railway-level issues. It provides guidance on some aspects of ensuring that railway systems work together to control risk, or, more specifically, on avoiding some common problems in this area.

When you connect together several systems to accomplish one objective it is unfortunately the case that the ensemble does not always do what you want, even though each system was built correctly, as far you could tell. As systems become more and more complicated, the likelihood of nasty surprises increases, unless you do something about it. This application note deals with three issues that arise when dealing with systems that are interconnected:

- Specifying systems to be safe (see section 2 below).
- Identifying, communicating and managing assumptions, dependencies and caveats (ADCs), which form an important part of the specification of a system's interface and functionality (see section 3 below).
- Modelling failure detection at the railway level, and taking proper account of it when assessing and controlling risk (see section 4 below).

Each of these issues is already addressed by one or more Yellow Book fundamentals. This application note does not attempt to place any new obligations on you. It provides practical guidance on implementing the fundamentals in the areas listed. It is intended to be read with the Yellow Book.

The note is primarily written for people introducing new systems (including those managing the work) or co-ordinating ESM activities at the railway level but may be useful to other people as well, such as independent safety assessors and safety authorities.

We have taken trouble to make this note accurate and useful, but it is only a guide. We do not give any form of guarantee that following the recommendations in this note will be enough to ensure safety. Although it provides guidance on good practice there may be other ways of tackling the problems described in this note which are not described here but are still good practice.

We are continually working to improve the Yellow Book and we welcome comments. Please contact us at the address below, if you have a suggestion for improvement.

The ESM Administrator
Praxis Critical Systems,
20 Manvers Street,
Bath BA1 1PX
UK

Tel: +44(0)1225 466991

Fax: +44(0)1225 469006

Email: info@yellowbook-rail.org.uk

2 SPECIFICATION ISSUES

2.1 The Problem

The *Defining Change* fundamental states that you “...must define the aims, extent, and context of the change.” You need to do this to ensure that the change will be safe in the context of the railway as a whole.

2.2 Guidance

When specifying a system you may find it useful to check that you have specified clearly for every aspect of the system:

- Its **function**

Not just what it does, but also what it must not do.

- Its **interfaces**

With other systems, and with people and the organisation.

- Its **environment**

Relevant parameters may include ambient temperature ranges, levels of electro-magnetic interference, and organisational aspects such as the level of training of users.

- The **quality of the service** it must provide

The standard to which the functional requirements are to be fulfilled. Relevant criteria include safety, reliability and availability.

- Other **contractual and related issues**.

Any relevant issues of intellectual property, licences, patents, spares, manuals and so on. If you do not take these into account you may find that they limit your ability to react to problems in the future.

Appendix A provides examples of what might be included under each heading. The Yellow Book Application Note on Software and EN 50128 also provides guidance on writing specifications which you may find useful even if you are not specifying software.

3 ASSUMPTIONS, DEPENDENCIES AND CAVEATS

3.1 Introduction

The safety of systems is not usually entirely in the hands of those developing them – safety is often reliant on other people’s actions as well. As a result, the developers find themselves making assumptions and placing dependencies and caveats.

Assumptions, dependencies and caveats are aspects of the interfaces between systems. Managing these assumptions, dependencies and caveats may be regarded as part of managing these interfaces.

Assumptions are made about the rest of the world, including the people and organisations with which it will interact as well as the physical railway. For instance certain tolerances on the supply voltage may be assumed. Someone will have to check that these assumptions hold when the system goes into service and continue to hold for the rest of its life (or deal with the situation if they do not). Assumptions are likely to be made throughout the project but many will be made near the beginning as input to the design process.

Dependencies are put on people, which means that they are required to act before the system can safely be put into service. A dependency is an agreement between you and another party that they will put something in place before the your system enters service. For example, if a computerised signalling system is being installed in a control centre, you may depend on someone else to upgrade the air conditioning first. Dependencies are likely to be placed throughout the project but many may not be placed until later in the project as they are likely to be outputs from design.

Caveats are placed on people. These are conditions that people must respect after the system is put into operation for it to remain safe. For instance, a certain inspection regime may be required. Caveats are likely to be placed late in the project, after detailed design has been done.

We will treat assumptions, dependencies and caveats together and call them ADCs for short.

Not all ADCs affect safety but many do. If they are not identified or are placed but not dealt with, a hazard may result

The diagram below illustrates some of the ADCs that may be placed for a new train.

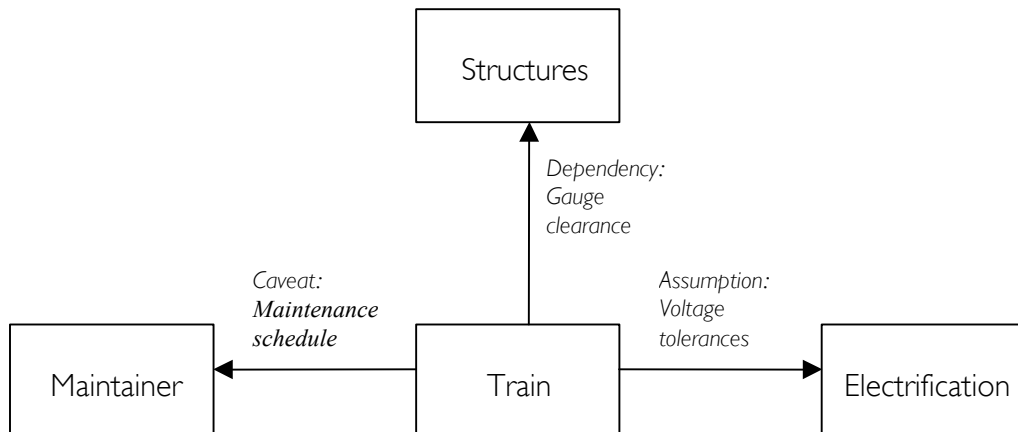


Figure 1 - Example Assumptions, Dependencies & Caveats

ADCs may be captured in standards, such as Railway Group Standards, and Technical Specifications for Interoperability. However, standards cannot capture all ADCs and just following standards is unlikely to reduce risk as low as reasonably practicable.

The railway has grown over many years without procedures for managing this information, and much of it has not been recorded. Moreover, it has been built by many different companies, adapting to different terrains, locations and environments, and different ADCs may be placed on similar systems in different places. ADCs for a line which is electrified will be different from those for one which is not.

If you place an ADC, you should make sure that it is understood and accepted by the people who will have to deal with it. This obligation is clear from the Yellow Book fundamentals for **Safety Responsibility** and **Communicating safety-related information**. Conversely, you need to make sure that you respect any ADCs placed on you.

3.2 Identifying ADCs that you will place on others

ADCs are identified as a natural by-product of activities at all stages of the system life cycle.

In particular, ADCs may be identified while defining the boundaries of your system and form part of the specification of the boundary of the system.

However, before you make an assumption, you should consider if it could be confirmed as a fact.

All ADCs which are relevant to the safety of the system are likely to form part of the safety argument at some point, so you should consider how you will resolve them when you make or place them.

3.3 Identifying ADCs that others will place on you

Failure to respect a safety-related ADC placed on you is likely to result in a hazard, so identifying ADCs placed on you is part of hazard identification.

You should consider all the other systems with which you might interact (whether on purpose or not) and look for ADCs they may place on you.

When looking for ADCs it is important to involve people with sufficient domain knowledge of the system as a whole and the environment, both physical and organisational, that the system must interact with. It is important to have not just those with specialist knowledge of small parts of the system, but also those with broader knowledge of the operation of the wider system.

If there are centrally co-ordinated registers of ADCs, you should consult them. They may be either at the network or regional level or by discipline, such as electrification and signalling. However, you should not rely on a central register as your only source.

The checklists on the Yellow Book web site for identifying hidden assumptions in risk models can also be used to identify ADCs on you.

3.4 Documenting ADCs

Within your organisation, you should adopt a consistent method of recording, naming and referencing ADCs in order to make communication and management simpler.

The storage and management of ADCs should not require excessive additional bureaucracy, or paperwork. Therefore you should attempt to integrate any method for the recording and management of ADCs with other parts of your process, and organisation.

ADCs may be conveniently stored in a register, which is part of, or kept, with the system's Hazard Log.

ADCs have a life cycle, from the moment that they are recognised and recorded, to the moment when they are either assigned to someone who understands and takes responsibility for them, or closed in some other manner.

You should have some system for recording the ADCs you place, the ADCs that other people place on you and tracking their progress. Where possible the status should be recorded with the original entry, or directly referenced to and from it.

As each ADC is identified, someone or some group of people who understands it should take responsibility for resolving it.

Resolving ADCs may involve coming to an agreement with people outside the project, for instance agreeing aspects of the infrastructure maintenance regime with a maintenance contractor or agreeing operating restrictions with a train operator. In some cases, resolving an ADC may have business implications in which case, whoever is responsible for this ADC should be in a position to handle this aspect of it.

Some centrally co-ordinated register or registers of ADCs held by the relevant railway authority (infrastructure controller or train operator) is desirable. If they exist then all projects should submit their ADCs to them. Where a central coordinating system is used, a single indexing and management process will improve the cross referencing of ADCs between projects.

Assumptions and caveats will also be present in the Safety Case in order to provide context to the safety argument.

If you use a specialist notation to represent your safety arguments, for example Goal Structured Notation (GSN) [1], Claim Structures (see appendix H of [8]), Toulmin [3], or the Adelard Safety Case Development Manual (ASCAD) [4], you may be able represent some or all ADCs directly in the safety argument using this notation.

Safety certificates will contain ADCs which the operator must monitor or act on. For example they may include assumptions about maintenance schedules.

3.5 Resolving ADCs

By their nature, ADCs are not normally fully closed by the project alone. The project's responsibility is to ensure that someone else understands and accepts each ADC. We say that an ADC is **resolved** when this has been done.

ADCs may be communicated in Safety Cases, Hazard Logs, correspondence, formal handover documents, operations and maintenance manuals ([2] 11.2, 11.6). If you need operations or maintenance staff to be aware of an ADC, you will normally deal with it in the operations or maintenance manuals. Typically this will be safety-related information which you will need to highlight as such. An ADC should not be considered resolved until the recipient has confirmed that they understand and accept responsibility for it.

The type of responsibility will be different for assumptions, dependencies and caveats. An assumption is resolved when someone takes responsibility for checking that it holds when the system goes into service and thereafter or dealing with the situation if the assumption does not hold. Dependencies and caveats are actions and are resolved when someone takes responsibility for carrying them out.

ADCs may initially be placed on those responsible for the installation and integration of the system with the railway as a whole and transferred later to those who are responsible for the ongoing management of the system.

However, before you pass on an ADC you should consider if you could design it out of your system. Reducing the dependency between systems is good systems engineering practice, and simplifies the integration of the system. You should weigh this against the effort involved and possible effects that such a redesign may have on the safety of the system. Designing out an ADC will not be appropriate in all circumstances.

It may also help to make the interfaces of a new system the same as the old one that it replaces. This may result in a more complex interface being used than could be developed from scratch. However, it may be easier to resolve the ADCs implicit in the interface.

ADCs should be examined regularly throughout the lifetime of the system to ensure that information about them is kept up-to-date and complete, that any new ADCs which have emerged have been dealt with and that existing ADCs are still valid.

Where two or more projects share an interface, regular meetings between them may be useful to resolve ADCs. Where a new system shares an interface with an existing system, meetings between the developers of the new system and those responsible for operating the existing system may similarly be useful.

In most cases some ADCs will be the responsibility of people within other organisations. When transferring responsibility to other organisations you may face problems: identifying those with sufficient skill, and assigning the responsibility to those people. You should make the transfer of responsibility part of your process for the handover of the project, working with clients and partner organisations to ensure that an appropriate person or group of people takes responsibility for each ADC. In some situations you may not be able to assign responsibility directly to an individual. It may be necessary to assign it to the organisation as a whole, with some individual, who may not have the skills or knowledge to deal with it directly, but takes the responsibility to ensure that it is dealt with by someone who does.

In general the assignment of responsibility is likely to be a difficult process and you will have to take a pragmatic approach. Most importantly, you must ensure that responsibility is never lost. It is better to have it transferred to someone who, while not equipped to take the responsibility directly, is in a position to assign it to someone who is.

4 FAILURE DETECTION AND MODELLING

4.1 Introduction

Many hazards are caused by failures that put the railway into a dangerous state. There are almost always mechanisms to detect the failure and mitigate the danger. Usually, for instance if both filaments of the red aspect of a signal fail, this is detected by the interlocking which will almost immediately set other signals red.

The fact that railway systems mitigate each other's hazards provides *network resilience*: the railway as a whole is safer and more reliable than any of the individual systems. This is not just a product of automatic functions only, communications systems may facilitate failure or emergency messages to be made in accordance with Rules and Regulations. The manner in which human beings and the organisation as a whole behave will affect the safety of the system.

It is possible to inadvertently degrade this network resilience if this is not recognised. For example, if an emergency is reported using a mobile telephone rather than a railway telephone, then the recipient may not have confirmation of the location of the person reporting the emergency.

The Yellow Book **Assessing risk** fundamental requires that "Your organisation must assess the effect of any proposed change on overall system risk". You need to take account of failure detection in two ways to do this.

- Firstly, you need to understand how the railway can detect and respond to hazardous failures of your system in order to estimate the **time at risk**, the time between entering and leaving the dangerous state. This can be a major factor in the assessment of the risk associated with the system. The risk associated with signal filament failure is generally assessed to be low, for instance, because the time at risk is short.

Chapter 8 of the Yellow Book describes the process by which you assess risk arising from a system using Cause and Consequence Analysis. As part of Consequence Analysis it is important to look for factors that can mitigate hazards. In many cases the ability of other systems, mechanical or otherwise to successfully mitigate a hazard will be dependent on the time taken to react. In order to assess fully the risk in the system, you need to be able to assess the time at risk, and decide the probability of an accident occurring during that time.

- Secondly, you need to understand how your system can reduce risk arising from other causes by detecting or mitigating hazards elsewhere.

4.2 Failure detection

You can reduce overall system risk by increasing the system's ability to detect hazards in the rest of the railway. However, when you remove an old system, you may also inadvertently reduce the ability of the network to detect failure. If you are replacing an older system you will generally wish to ensure that the new system is at least as capable of detecting hazards as the old one. If you cannot achieve this then you should look for measures that can be taken to compensate for the loss of network resilience. It is important that the *overall* safety of the network is not reduced; any loss of failure detection should be weighed against possible improvements in safety that may result in an overall improvement.

4.3 Modelling failure and its detection

In order to understand the effect that a change will have on the safety of the system, it is important to identify those systems that have dual roles, both functional and safety. You should identify how the system that is being modified may provide safety functions to the network as a whole. You should characterise how it behaves when faced with potentially hazardous sequence of events and how quickly it reacts. You should identify the manner in which the railway as a whole reacts to the failure of a single component.

Where an existing system is being replaced, it may be possible to use the results of hazard analysis carried out on the original in order to understand how it relates to other systems in the event of a hazard. You should examine the interfaces of the existing system to identify the systems (including such things as track) with which it interacts, and identify the failure modes of these systems.

In all the examinations of the interaction of the system with the railway as a whole, you make use of the ADCs of the system. Through them you can identify the manner in which it interacts with the other parts of the railway.

Failure scenarios can be complex. The railway may pass through several unsafe states, before returning to a safe one, each transition potentially being the result of a different system. State-transition diagrams and UML can provide useful notations for capturing these scenarios.

Figure 1 (below) is an example state transition diagram. The round cornered boxes represent the states of the system, and the arrows represent the transitions between those states. This example models debris being on a track, and the driver of a train on the neighbouring track spotting it, and notifying the control centre. All the states within the box are ones for which the railway is at risk.

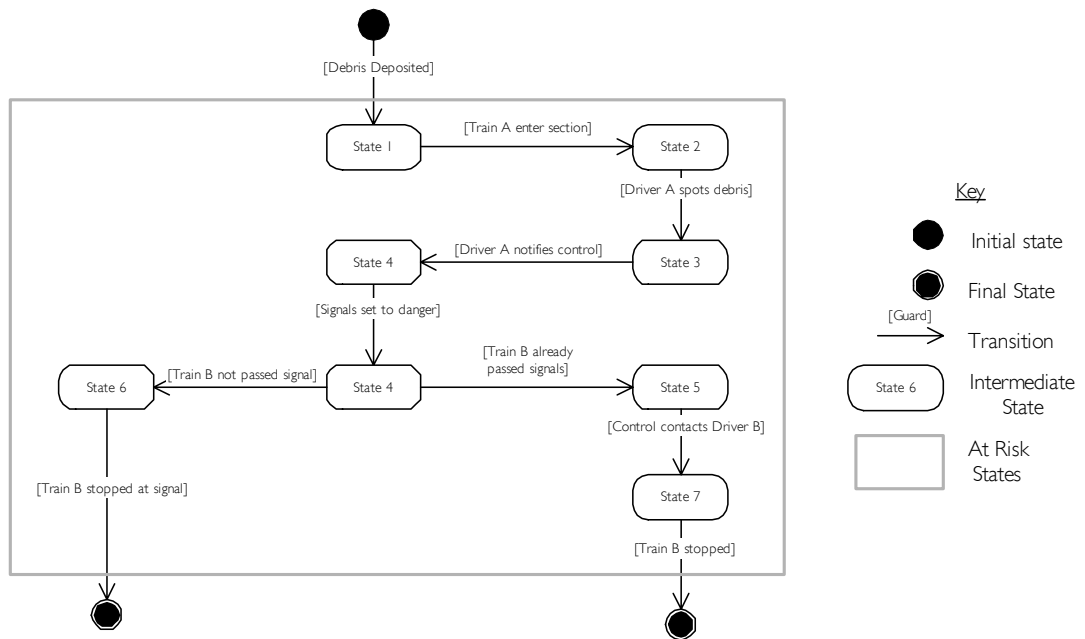


Figure 2 - Example State Transition Diagram

4.4 Estimation of time at risk

In some cases, it may be sufficient to make a single point estimate of the time at risk, based upon the most likely scenario for making the railway safe. It is acceptable to be approximate provided that approximations are conservative, that is that they do not under-estimate risk (see Yellow Book 3[2], volume 2, paragraph 8.4.3).

If you have modelled failure scenarios using state-transition diagrams, you can use these to estimate time at risk. In the simple case where there is only one sequence of events, a single estimate of the time spent in each state may be calculated. Markov models may be used to make a statistical estimate of time at risk in more complex situations.

5 REFERENCED DOCUMENTS

- 1 Arguing Safety – A Systematic Approach to Managing Safety Cases, T.P. Kelly, University of York – Department of Computer Science, 1998.
- 2 Engineering Safety Management, issue 3, Yellow Book 3, Railtrack, 2000.
- 3 Toulmin, The Uses of Argument, Cambridge University Press, Cambridge 1957
- 4 <http://www.adelard.co.uk/resources/ascad/>
- 5 Defence Standard 00-56, Issue 2, 13 December 1996, Safety Management Requirements for Defence Systems
- 6 EN 50126, Railway applications - The specification and demonstration of Reliability, Maintainability and Safety (RAMS), 1999
- 7 ENV 50129, Railway Applications – Safety Related Electronic Systems for Signalling, 1998
- 8 Defence Standard 00-55, Requirements for Safety Related Software in Defence Equipment, 1997

6 ACKNOWLEDGEMENTS

This guidance was prepared with the help of the following people who provided their time and expertise as professionals committed to improving railway safety. Their views do not necessarily reflect those of their employers. Their contribution is gratefully acknowledged.

Richard Allan, Railtrack
Andy Bourne, London Underground Limited
Bob Brewer, Praxis Critical Systems Limited
John Corrie, Mott MacDonald
Paul Cheeseman, Lloyds Register MHA Limited
Stephen Denniss, Bechtel
Bruce Elliott, Praxis Critical Systems Limited
Ali Hessami, WS Atkins Rail Limited
Paul Leader, Praxis Critical Systems Limited
David Waboso, Nichols

John Corrie initiated this application note and provided technical leadership when writing it.

A APPENDIX: EXAMPLE SPECIFICATION TOPICS

This appendix takes the specification checklist of section 2.2 and provides examples of topics that might be addressed in the specification of a railway control centre.

- **Its function**
 - Facilitate operation to the timetable
 - Provide capacity for agreed levels of service recovery
 - Provide control facilities under failure and emergency conditions and their recovery
 - Enforce the safety principles
 - Protect staff
 - Provide fault alarms and operation logging
 - Provide customer and management information
 - Facilitate efficient use of traction energy
- **Its interfaces**
 - Organization (operators, maintainers, management, customers, emergency services)
 - Trains (human drivers or automatic systems, train protection, vehicle health monitoring)
 - Way (train detection, points, indicators, bridges, tunnel ventilation etc)
 - Electrical traction power (supply distribution control)
 - Neighbours (level crossings, other railways)
 - Station and terminal services, depots, technical (positional references, loadings, earthing policy, heat dissipation)
 - Chemical interfaces – (dissimilar metals)
 - Data formats and information flow
- **Its environment**
 - Organization (staff competence – select, train, resource, authorize, motivate, monitor)
 - Railway rules and procedures
 - Weather
 - Shock and vibration
 - Electromagnetic interference
 - Noise
 - Local conditions and lighting
 - Faulting and maintenance support policy
 - Vandalism/terrorism/malicious acts

- The **quality of the service** it must provide
 - Safety
 - Reliability
 - Availability
 - Maintainability
 - Economy
 - Service life (stating how this will be accepted)
 - HMRI approval
 - Industry and other standards and norms (themselves functional)
 - Train service quality management
 - Targets (train paths provided, delays, recovered energy, efficiency, costs)
 - Public perception

Additionally, for adapting existing railways while traffic continues to run, the quality of the service provided (operated and supported by staff of stated competence) during staged introduction of new systems.

- Other **contractual and related issues**
 - Patents and copyright
 - Licences (jigs, tools, templates, software use and alteration)
 - Spares and special test/diagnostic equipment
 - Documentation and manuals
 - Certification
 - Training

Published in December 2002 by:
Railway Safety
Evergreen House
160 Euston Road
London NW1 2DX
Phone: +44 (0)20 7904 7518
www.railwaysafety.org.uk

Distributed by:
Praxis Critical Systems Limited
20 Manvers Street
Bath BA1 1PX.
Phone: +44 (0)1225 466991
www.praxis-cs.co.uk

Copyright © Railway Safety 2002
Cover photograph copyright © Milepost 92½ 1995

You can download further copies from:
www.yellowbook-rail.org.uk