ATOC-RIA TTT

Association of Train Operating Companies - Railway Industry Association

Issue 1 – September 2004

Approved Code of Practice – The Elements of Management of Safety Critical Components on Trains

Submitted by:

Richard Gostling – Railway Industry Association

Jon Leigh – SABWABCO

John Collins – Angel Trains

Stephen Ford – Bombardier Transport

Dominic Dent - ATOC

Ian Duncan – First Great Western Link

Ian Mylroi – ScotRail

Synopsis

To facilitate the management of Safety Critical Components by Train Operating Companies and Suppliers/Manufacturers.

Authorised by:

Richard McClean, Chair of ATOC Engineering Council

Contents

Part A

Issue Record

This Approved Code of Practice will be updated when necessary by distribution of a complete replacement.

Amended or additional parts of future revisions will be marked by a vertical black line in the adjacent margin.

Issue	Date	Comments
Draft	May 2004	Original draft
Draft 2	July 2004	Amendments to original draft
Draft 3	August 2004	Amendments to draft 2

Explanatory Note

This technical publication was produced by a working group tasked with improving the management of Safety Critical Components, and set up by ATOC (the Association of Train Operating Companies) with TOCs, & RIA (Railway Industry Association), with ROSCOs (Rolling Stock Companies) and Suppliers/Manufacturers under the banner 'ATOC-RIA Transforming Trains Together' (ARTTT).

It is to be disseminated and used within the railway industry. We intend to review its effectiveness after one year of operation i.e. in August 2005 – in the interim please send any feedback to rebeka.sellick@atoc.org or rgostling@ria.org.uk.

This publication is not a mandatory standard. Whilst ATOC Approved Codes of Practice are intended to disseminate best practice, users must evaluate this technical publication against their own requirements in a structured and systematic way. Some parts of it may be decided not to be appropriate at the user's discretion. It is recommended that the evaluation and decision to adopt (or not to adopt) this publication is documented and reviewed from time to time.

Code of Practice Status

This document is not intended to create legally binding obligations between companies and it shall be binding in honour only.

Supply

Controlled and uncontrolled copies of this Approved Code of Practice may be obtained from Serco Raildata.

Part B

1.0 Purpose

ATOC, RIA, Suppliers/Manufacturers and TOCs have co-operated to produce this Code of Practice. It is designed to improve the management of Safety Critical Components.

2.0 Scope

This ACOP applies to Safety Critical Components used on trains.

3.0 Definitions

Engineering Change	A proposed alteration to existing train or component designs, maintenance or manufacturing processes or procedures, suppliers or supply arrangements, which has the potential to impact on the safe operation or asset life of T&RS. This is as specified in ATOC ACOP/EC/1006 Management of Engineering Change.
Owner	The person or organisation who legally owns a product, patent or manufacturing rights to a vehicle or component
Railway Safety Case (RSC) Duty Holder	The professional Head of Engineering of a Train Operating Company or his/her representative.
Railway Group Standards	Standards issued by Railway Safety and Standards Board (RSSB) or any successor body affecting the Duty Holder.
Safety Critical Components	Components, systems or sub-systems which have the potential to fail and directly threaten health and safety.
Suppliers/Manufacturers	Any Supplier or Sub-supplier of Safety Critical Components to a RSC Duty Holder, which includes any party who manufactures, overhauls, repairs, inspects, tests or handles Safety Critical Components.
Third Party Modifications	Modifications developed/undertaken by a company who is not the original component manufacturer.

4.0 Abbreviations

ARTTT	ATOC-RIA Transforming Trains Together
ATOC	Association of Train Operating Companies
AWS	Automatic Warning System
BR	British Railways
EU	European Union
HMRI	Her Majesty's Railway Inspectorate
IPR	Intellectual Property Rights
OEM	Original Equipment Manufacturer
PADS	Parts And Documentation System
RIA	Railway Industry Association
TPWS	Train Protection and Warning System

5.0 Introduction

5.1 Why improve the management of Safety Critical Components

Sound and economic management of Safety Critical Components is of core importance to the railway, and existence of both new and a large number of older or modified subsystems generate particular issues.

These issues are described in a number of specific cross-industry codes of practice, for which this document seeks to provide an overarching framework; consistent with the responsibilities of RSC Duty Holders in particular, and of suppliers generally.

5.2 Key Elements

Successful management of Safety Critical Components requires the following elements:

- identification that the component is safety critical;
- explanation of why the component is safety critical;
- documented initial design;
- proven initial design;
- identified holder of the 'Know-Why' of the design ('The Engineer');
- definition of required performance (which cannot be greater than for the initial design, without design change);
- specification of detailed overhaul processes, including test regimes;
- component through-life traceability, where appropriate.

For older trains, some of the elements may not be formally recorded, the overhaul specification may be based upon good current practice, and IPR ownership may be unclear or may have passed to other parties through component development.

For new trains, these elements, and the associated IPR, are likely to be concentrated in the OEM and train builders.

In either case, subsequent changes, which may affect performance capability or reliability, or the cost of overhaul, are likely to require modified versions of these elements. If any of these elements are modified, an Owner should (i.e. recommended, but not mandatory) be identified for each component changed.

This document presents an overview of the key factors associated with each of these elements, and provides reference to specific documented processes and principles developed through ARTTT, and elsewhere, as shown in the diagram in appendix 11.3.

6.0 Identification of Safety Critical Components

This is the responsibility of each RSC Duty Holder (1,2), according to the following principles:

- Whether or not a particular item is safety critical depends upon application, and;
- any item identified as safety critical by one RSC Duty Holder is (for ease of management) treated as safety critical for the others;
- safety critical items should be identified in PADS, with all users listed, and cannot be deleted from PADS, nor their safety critical status amended, without agreement of all users;
- for new trains, items may also be identified in the manufacturers' system;
- third party modification of old or new train components will be outwith the initiating design 'Know-Why' and should be referenced in PADS.

6.1 Explanation of why the Component is Safety Critical

Explanation of the logic for designating a component safety critical has three purposes:

- to enable suppliers to manage the risks associated with each component down to a level acceptable to RSC Duty Holders;
- to facilitate informed discussion for multiple user items;
- to avoid confusion when items are proposed for deletion from PADS.

7.0 Documented Safety Critical Design

Every safety critical design should be documented in a coherent database, with a unique part number.

For existing designs, the relevant data is held in PADS, which will be suitably modified, including taking into account its position as a repository of safety information.

For new designs, the complete parts lists, together with related drawings and documents, are normally held by the train builder. Safety critical parts are also listed in PADS.

Where parts are modified in a way which affects performance (fit, form or function), or which is irreversible (eg enlargement of bores), then the resulting part requires new part (and where appropriate catalogue) numbers which need to be recorded.

If the change is made outside the OEM's system, then the new part details need to be recorded in PADS.

7.1 Holder of the Design Know-Why

Design 'Know-Why' (3) is fundamental to successful Engineering Change (4), and for each item it should be possible to identify the holder of the 'Know-Why', which should be recorded in PADS to the satisfaction of the RSC Duty Holder.

Where an Engineering Change requires 'reconstruction' of the 'Know Why', this requires a different catalogue number, and the new holder of the 'Know-Why' becomes the authoriser of the revised documents/drawing referred to in PADS. If reconstruction of the 'know-why' is needed and the OEM is still in existence, OEM co-operation in assisting in establishing and documenting best practice is requested. In these cases, a balance should be drawn between capturing best practice for the industry and preserving sensitive IPR.

8.0 Proven Design and Re-design

Prior to 1994, trains were certified by internal BR processes, and (latterly) accepted for operation by HMRI.

New trains are currently certified under the ROTS Regulations (5), but progressively from the end of 2004, all new trains and significant modifications to existing trains will be certified under the EU Interoperability Legislation (6,7).

Engineering Changes to component design whether made by the OEM or otherwise require that:

- the relevant parties are appropriately involved ;
- the 'elements of design authorities' are properly addressed (3);
- the level of proof of design is sufficient (normally at least equal to that initially applied, unless decided otherwise).

9.0 Overhaul Specifications

For all trains, there will be a defined maintenance plan – part of which will identify those components requiring overhaul. The precise overhaul requirements (i.e. the detailed work to be undertaken) shall always be defined in a "prescriptive" specification, with the IPR owned either by the customer/Owner or the supplier depending on the contractual relationships and who is the holder of the design 'Know-Why'.

Sometimes an additional "performance" specification is required, which defines the target performance of the component (in terms of reliability, life, expected duty cycle etc) and would form the contractual relationship for the overhaul.

Some examples of how overhaul specifications are implemented are given below:

- The overhaul of new trains is often carried out by the train manufacturer or OEM and defined in a prescriptive specification (defined by the train manufacturer or OEM) and a performance specification forms the contractual document;
- The overhaul of older trains is often carried out by the train owner or operator and is defined in a prescriptive specification (often developed from ex BR Common Domain documentation by industry consensus). In this case the prescriptive specification is often the contractual document, with any performance targets included for reference only;
- The overhaul of modified equipment or introduction of a new overhauler has a range of different contractual arrangements which may include the above examples.

Regardless of its ownership, overhaul documentation shall be made available for audit purposes as required.

The status of every specification for a Safety Critical Component is to be recorded in PADS. Enquiries relating to Safety Critical Components will be available to all parties, but data may only be changed by authorised bodies (typically the document owner or holder of design 'Know-Why'). See Appendix 11.2 for summary of PADS functionality in relation to component information management.

Industry best practice for developing and writing new technical documents is defined in CR/DT0001 (8). The principles of CR/DT0001 should be applied to suppliers' internal processes and these should also be auditable.

10.0 Traceability

For some components, traceability of the life history is important, e.g. to ensure that fatigue life is not exceeded or to identify repeated faults. The tracking system developed through ARTTT for one particular group of components (selected from AWS and TPWS systems) is described in (9).

11.0 Appendix

11.1 References

1 RGS: GM/RT2450 – Qualification of Suppliers of Safety Critical Engineering Products and Services

2 ACOP/EC/01003 – Approved Code of Practice – Supplier Accreditation Scheme

3 RGS: GE/GN8565 - Guidance on the Retention of Design Information for the Validation of Technical Change and Configuration Management

4 ACOP/EC/01006 – Approved Code of Practice – Inter-Company Train Engineering Change Approval Process

5 Railways and Other Transport Systems (Approval of Works, Plant and Equipment) Regulations, 1994

6 Regulations Implementing the High Speed Interoperability Directive (June 2002)

7 Regulations Implementing the Conventional Interoperability Directive (expected to be published Summer 2005)

8 CR/DT0001 – Production of Technical Publications

9 ACOP/EC/01001 – Approved Code of Practice – AWS/TPWS Component Life Instructions

11.2 PADS functionality in relation to component information management

Data	Requirement
Safety Criticality of Components	Identify if YES / NO or NOT ASSESSED. If Safety Critical display a 2-character RAVERS code indicating system and sub-system and which TOC initially flagged the component as safety critical
Components General Information	Holder of know-why responsible for controlling information changes on PADS. TOCs using component (based on advice from TOCs) Vehicle Classes using component (based on advice from TOCs). Applicable Documents and Drawings relating to definition or overhaul of the component.
Documents and Drawings	Document or drawing owner. Identify if these directly relate to definition or overhaul of safety critical components. Identify if through audit or some other means the document or drawing has been flagged as requiring review (details to be entered in freeform).

PADS will be updated when document references or part numbers are changed.

11.3 Document Hierarchy