Specification: ETCS Reference Design Hazard Assessment Support

This Tender is issued by:
Rail Safety and Standards Board
RSSB
www.rssb.co.uk

1. Background

1.1. The National ETCS Development Team (EDT) is developing a National ETCS solution for application on the GB railway. This covers a variety of Network Rail's programmes and projects, and ETCS suppliers.

1.2. As part of this exercise a reference design is currently being developed from which requirements will be extracted into the System Requirements Specification (SRS).

2. Purpose

2.1. Introduction

2.1.1. The EDT has requested help to carry out hazard analysis and assessment activities in support of the developing reference design. The work is intended to address the following areas:

i. Identify hazards associated with delivering the reference design proposal on an operational railway in GB;

ii. Qualitatively assess those hazards,

iii. Record the design assessment and justification for any discounted design options;

iv. Identify measures to reduce or mitigate these hazards;

v. Determine both with and without identified mitigations, whether risk from the identified Hazards is likely to be controlled to an acceptable level.

vi. Deliver the above in compliance with the requirements of legislation including CSM REA (Common Safety Method on Risk Evaluation and Assessment).

3. Scope of Services

3.1. General description

3.1.1. The remit requested the following key activities be undertaken involving system experts and key stakeholders:

i. Activity 1 – Hazard Identification and assessment

ii. Activity 2 – Hazard Mitigation identification and assessment

iii. Activity 3 – Determine whether risk from all identified hazards associated with the proposed reference design is likely to be controlled to an acceptable level.

3.1.2. These are key stages in the required process of delivery of the ongoing CSM risk assessment process for implementation of ETCS as described below:

i. Define the ETCS system to be studied, including identifying existing requirements

ii. Identify ETCS Hazards

iii. Identify existing risk control measures

iv. Classify the Hazards in terms of their expected frequency and consequence (preliminary risk ranking)

v. Preliminary risk evaluation to understand the sufficiency of the risk controls currently included in the system definition

vi. Identify further measures that are likely to reduce or mitigate Hazards to an acceptable level where necessary

vii. Evaluate the residual risk, taking account of additional identified mitigation measures

viii. Record results of the risk assessment process, including any assumptions, dependencies, caveats, issues and open points for continual hazard management (e.g. create a Hazard Log).

3.1.3. The steps above are designed to fit into the follow-on activities below, undertaken by the EDT:

i. Revise System Definition to take account of new controls/safety requirements and any other new information

ii. Repeat the Risk Assessment process for the revised System Definition (iterative process)

iii. Undertake whole system HAZOPs to review interactions between and interfaces between the facilities previously studied.

3.1.4. This approach is in line with the requirements of the CSM REA and is consistent with the ERTMS National Programme – Industry Safety Strategy.

3.1.5. The NR Safety Plan for the ETCS Programme is currently being developed and will be forwarded when available.

3.2. Common Safety Method on Risk Evaluation and Assessment

3.2.1. EU Legislators approved the Railway Safety Directive 2004/49/EC in 2004 to support efforts to harmonise European railways and create a single market for services and supply while maintaining safety. This Directive introduced the requirement for a Common Safety Method on risk evaluation and assessment (CSM REA), which came fully into force in July 2012.

3.2.2. Application of the CSM REA is legally required for all significant technical, operational or organisational changes to the railway. It sets out a harmonized framework for the risk assessment process. The regulation sets out three risk acceptance principles: acknowledged codes of practice, similar reference systems and explicit risk estimation (in GB this is generally interpreted using the ALARP principle).

3.2.3. The structure of the CSM framework can be seen In Appendix A. The ORR has published guidance on the application of the CSM REA. RSSB has produced practitioner level guidance aimed at those who are required to undertake an application of the CSM REA process. The work carried out for ETCS will follow these guidelines to the appropriate level of detail.

3.2.4. The Hazard Analysis activities currently proposed represent a first pass through the early stages of the CSM risk assessment process which should be considered as an ongoing and iterative process and which will develop as the system design/definition becomes better developed. The associated hazard log should form foundation material for ongoing CSM safety activities at both a national programme level and for future specific implementation projects.

4. Detailed Description

4.1. HAZID process

4.1.1. The HAZID process shall be compliant with Rail Industry Guidance Note GE/GN 8642 "Guidance on Hazard Identification and Classification".

4.2. Activity 1 - Hazard Identification

4.2.1. Hazard identification shall be compliant with Rail Industry Guidance Note GE/GN 8642 "Guidance on Hazard Identification and Classification Section G3.5".

4.2.2. The HAZID activity shall be based upon workshops with system experts, using guidewords to provide an ordered approach to identify potential Hazards and to agree them with NR's representative.

4.2.3. RSSB strongly endorse the plan to implement a systematic approach to identifying hazards and mitigations. However, we believe that it is important to balance the desire for a rigorous and detailed approach with the need for a pragmatic approach that is suitable for the level of system definition currently available and recognises the constraints of potential open points and assumptions. A full scale formal HAZOP may be inappropriate at this stage (but may be suitable in a later iteration), and so a more flexible HAZID approach will be used, based on the same underlying safety management principles. The HAZID work will be carried out to a level that is appropriate to the level of detail in the current "system definition" material and the required timescales.

4.2.4. Hazards and control measures will be qualitatively assessed to produce material which can be used to inform an ALARP decision. This will generally be undertaken by the Suppliers following the HAZID workshop, based upon the consequences and controls identified, unless any hazard is believed by the workshop members to be important to classify during the workshop.

4.2.5. Responsibilities for provision of elements necessary to the process are detailed in Table 1, below.

4.2.6. They are split into:

- Supplier;
- RSSB;
- EDT.

Provided by	Supplier	RSSB	EDT
HAZID Chair person	✓		
HAZID Secretary (Note 1)	✓		
Technical & Operational Experts in ETCS facilities		✓	✓
Human Factors experts		✓	✓
Reference Design per facility			✓
HAZID input template		✓	
Risk Matrix			✓
HAZID report template		✓	
HAZID Briefing note	✓		
Risk Scoring	✓		
Completed HAZID input table	✓		
HAZID report per topic	✓		

Table 1: Responsibilities for Provision of Elements of HAZID Scope

Note 1: Any variation to the above shall be highlighted in the Tender Response.

4.3. Activity 2 - Hazard Mitigation

4.3.1. Existing risk control measures shall be recorded as part of the HAZID process and potential new control measures will also be identified where necessary.

4.3.2. A risk matrix approach will be most appropriate to provide a framework for the qualitative classification of hazards at this stage. This will help to ensure that subsequent work is focused on the most important risks and help to inform safety decisions.

4.3.3. Templated risk acceptance arguments shall be produced in the context of the CSM REA framework by the application of one of three risk acceptance principles: codes of practice, similar reference systems or explicit risk estimation. Workshops shall be used to elicit an initial assessment of the sufficiency of existing and potential controls. Further more detailed work may be needed and it is ultimately a requirement on the ETCS Implementation projects to ensure that each particular application of ETCS is acceptably safe.

4.4. Activity 3 – Determine Required Mitigation and Other Options

4.4.1. The output from the HAZID workshops and follow-on work shall generate a full list of risk control measures, indicating possible new requirements to ensure risk has been controlled to an acceptable level.

4.4.2. A preliminary qualitative analysis of the identified hazards and associated control mitigations will be carried out to a level consistent with the Reference Design at this stage; where possible, conclusions on which mitigations are required to reduce the risk to an acceptable level will be considered, in line with CSM safety management principles.

4.4.3. Qualitative consideration will be made on the required level of mitigation in line with CSM safety management principles, producing material to understand the residual risk and to inform the safety decision making processes of the EDT governance bodies (OSG and ESB).

4.4.4. Assumptions, dependencies, caveats and issues shall be clearly recorded and shall be traceable to each identified hazard.

4.4.5. Following the workshop all hazards shall be ranked both pre- and post-controls, in accordance with the Risk Matrix supplied in the Hazard Input spreadsheet.

4.4.6. The baseline assumed for hazard frequency shall be stated in the HAZID workshop report.

4.5. Context within the National ETCS Programme

4.5.1. Each ETCS topic is known by the term "Facility". Examples are "Entering ETCS", and "Level Crossings". Each Facility document describes the means by which the ETCS Reference Design will manage the function described. The reference design is developed and reviewed by the ETCS community. Once the document is passed by the Operations and System Boards, it becomes a "Working Version".

4.5.2. Changes are possible with Working Version documents, as the application of ETCS to the UK main line railway is still under development, but the review process described above prior to issue of the Working Version is designed to minimise the impact of such changes.

4.5.3. There are four work streams that each facility goes through once it has achieved Working Version status:

- The operational scenarios workshops;
- Review by ETCS supplier community;
- Review by NR IP/route community for first deployment projects;
- Safety assessment - led by RSSB.

4.5.4. The outputs from these four work streams are then assessed to determine how to update the facility to produce a new endorsed version from which robust requirements can be extracted.

4.5.5. A series of HAZIDs have taken place for which final reports have been submitted by the suppliers managing those HAZIDs. The associated reports and Hazard Logs have been accepted by the Network Rail EDT.

4.5.6. The next stage in the process is to undertake a further series of HAZIDs on related and new facilities.

4.5.7. The planned series of HAZID workshops are part the Safety Assessment stage above. The current list of facilities comprises a series of workshops planned to support the National ETCS Programme.

4.5.8. The current list of workshops covered are:

Facility	Title	Estimated workshop length (in days)	Work Package (WP)	Joint workshops	Reference design status
JJ	Level crossing management	2	WP1	N/A	Draft
R	Boundaries	1	WP2	i. Joint Workshop	Working Version
KK	Transmission of national values				Working Version
Y	Gradient and speed profiles	1	WP2	N/A	Working Version
Z2	Control of DMI units	0.5	WP3	N/A	Working Version
LL	Track conditions	0.5	WP3	N/A	Working Version
HH	Train maintenance facilities	0.5	WP3	N/A	Draft non-objected by OSG
CC	Packet 44	0.5	WP4	k. Joint Workshop	Draft non-objected by OSG

Facility	Title	Estimated workshop length (in days)	Work Package (WP)	Joint workshops	Reference design status
II	Balise rules				Working Version
AA	Consistent provision of lineside signage	0.5	WP4	N/A	Draft non-objected by OSG
U & S5	Route not proved and route proving	1	WP4	N/A	Draft
1-4	Up to 4 Contingency HAZID workshops of the same kind are included in the HAZID programme.	1 per workshop	1 per work package	N/A	To be defined

Table 2: Facilities Subject to HAZID

4.5.9. The planned length of workshops is 5h for a full day and 3h for a half-day.

4.5.10. Progress meetings between RSSB, EDT and the Suppliers will be held; it is envisaged that these will be held monthly, and that one representative from each Supplier should attend.

4.6. Work Packages (WP)

4.6.1. Each Facility is the subject of a HAZID; in some cases, the Facilities are part of a Joint Workshop, where this has been advised by EDT.

4.6.2. The Facilities have been grouped into Packages, based upon the length of workshops envisaged by EDT. Suppliers may bid for some or all of the Packages. The work is envisaged to be let to at least two Suppliers, to permit parallel development.

4.6.3. Reference designs for the Facilities to be subjected to HAZID are listed in Appendix A.

4.6.4. Exchange of Facility topics between packages may be necessary, dependent on stakeholder feedback. Wherever possible, the exchange will be made for topics of the same notional length.

4.7. Feedback from Previous Workshops

4.7.1. Feedback from analysis of the reports and Hazard Logs from the earlier workshops have been used to update the templates issued with this Invitation to Tender (RSSB1930ITT). Lessons learned from use of the HAZID forms used to develop the Hazard Log are collated in the Table below.

Ref	Title	Description
1.	Use of Hazard Description	The Hazard Description in each hazard sheet should be completed
2.	Risk scoring pre- and post-mitigation	The frequency and consequence scoring should be checked to reflect any mitigation applied - with mitigation the risk

Ref	Title	Description
		score would normally change unless there is a specific explanatory note.
3.	Recording non-key issues	Non Key issues should be explored and recorded as well as those with greater impact
4.	Checking whether issues are covered by other scope	NR, in consolidation of the Hazard Analysis Reports (HARs), have found that some actions will be addressed by other (degraded mode operation) workshops.
5.	Defining roles of HAZID participants	Distribution lists should include all reviewers.
6.	Applicability of specific conclusions to topics	Where conclusions refer to a topic sub-set, this should be made clear
7.	Risk ranking	All hazards should have a risk ranking
8.	Identification of blank forms	If any non-mandatory form is left blank, add text to say "Not Used"
9.	Use of term "driver training" in New Safety Measures	State what the driver training is expected to cover eg "Driver Training to cover ETCS constraints in attaching/detaching"
10	Inconsistent consideration of brake application safety measure.	In some cases the primary consequence has been considered to be the brake application leading to potential sudden movement / passenger injury. Whilst brake applications might be listed as a mitigation there is no change in pre and post mitigation risk scores. Alternatively, the brake application is considered as a secondary consequence resulting from the mitigation of brake application. The primary hazard is then more usually collision or derailment. The impact is that it reduces importance of initial hazard and reduces impact of [existing design] mitigation. Recommendation: Brake application to be considered as a secondary consequence and listed as a mitigation. Primary consequence would be whatever would occur if the brake application was not present. This should be reflected in the pre and post mitigation risk scoring. OR: Existing Mitigations considered to modify Primary consequence.
11	Crossover seen between the use of Hazard scenario and Hazard Description	Consistent common Hazard Titles should be adopted to enable Hazard Grouping: - Overspeed - Exceeds MA

Ref	Title	Description
		- ETCS Protection reduced - Non ETCS protection reduced.
12	Some crossover observed between the fields: HAZID Action, Hazard Title, Hazard description, Hazard Causes	Levels of information included (which will aid in understanding the nature and causes of the hazard) vary. Consistent common Hazard fields should be adopted.
13	Primary / Secondary consequence: Level of detail versus 'Hazard Description'	In some cases the consequence is described in significant detail and includes a chain of events to get to the final state - Detail is best put into the 'Hazard Description'.
14	Description of Safety Measures as New or Existing	Safety measures built into the ETCS design such as Brake Application are sometimes considered to be NEW (they were not there before ETCS) or EXISTING (They are planned as part of the design and there is no need to introduce an additional safety measure). Any safety measure that is already considered to be part of the ETCS design (i.e. within the system design spec / reference designs) should be considered as EXISTING.
15	Assumptions listing	In some cases, more than one assumption listed per assumption number Consistently used to list expectations of what other HAZID session should be covering. Also used in some instances to state that a particularly scenario does not present a hazard. Only one assumption to be listed per assumption reference number.

Table 3: Lessons Learned from HAZIDs

4.8. Not in Scope

4.8.1. Competence of HAZID attendees already determined, through experience of previous workshops. Setting up of workshops and organising availability of attendees is undertaken by RSSB.

4.8.2. Coordination of consistency between workshops is undertaken by RSSB.

4.8.3. Project templates are provided by RSSB. Templates for the HAZID Input Form (with macro) and for the HAZID Report are provided in Appendix A; these have been updated to reflect the Lessons Learned in Table 3.

5. Supplier Deliverables

5.1. Deliverables

5.1.1. The supplier shall be responsible for leadership, facilitation and recording of HAZID workshops within their respective work package, in accordance with the agreed programme. On the basis of these, the supplier shall provide the following deliverables:

i. A briefing note shall be provided for each workshop.

ii. A final Hazard Analysis report for each topic area identifying the following:

iii. Agreed Hazards and an initial qualitative assessment of the associated risk;

iv. Measures judged necessary to control risk to an acceptable level;

v. Record of the design assessment and justification for any discounted design options;

vi. Measures considered but not judged necessary to control risk to an acceptable level;

vii. Any impact assessments necessary to support mitigations;

viii. Any suggested further work, or open points requiring resolution

ix. A key output of the Hazard Analysis report will take the form of a HAZID Log delivered in a format which allows for future development and expansion as appropriate. The form and content has been be agreed with the EDT

x. The supplier shall complete the qualitative risk assessment and ranking of each hazard within the hazard log in accordance with the supplied risk matrix

xi. The hazard log shall include tabs for assumptions, dependencies, caveats and open points for further reconsideration.

5.1.2. Both the Report and the Hazard Log shall be submitted in editable format. The Report shall also be submitted a signed document in Adobe Acrobat.

6. Timescales

6.1. Overall Programme

6.1.1. In order to coordinate with the already programmed production of batches of facilities, the HAZID workshop programme should be commenced as soon as reasonably practicable.

6.1.2. A preliminary review of the structure and assumed content of batches of facilities and options suggests a requirement for approximately nine workshop HAZID studies, in addition to four contingency workshop HAZID studies, of varying complexity and duration, as described in Table 2. If the production programme for batches 1-6 is adhered to, it is understood that these workshop/desktop studies are required to be completed over the period running 10 June – 30 September 2015.

Work package 1	40 days	10/06/15	04/08/15
Topic 'JJ Level Crossing Management'	40 days	10/06/15	04/08/15
Work package 2	55 days	10/06/15	25/08/15
Topic 'R Boundaries' & 'KK Transmission of national values'	40 days	10/06/15	04/08/15
Topic 'Y Gradient and speed profiles'	40 days	01/07/15	25/08/15
Work Package 3	70 days	10/06/15	16/09/15
Topic 'Z2 Control of DMI units'	40 days	10/06/15	04/08/15
Topic 'LL Track conditions'	40 days	01/07/15	25/08/15
Topic 'HH Train maintenance facilities'	40 days	22/07/15	16/09/15
Work Package 4	70 days	10/06/15	16/09/15
Topic 'CC Packet 44' & 'II Balise rules'	40 days	10/06/15	04/08/15
Topic 'AA Consistent provision of lineside signage'	40 days	01/07/15	25/08/15
Topic ' U & S5 Route not proved and route proving'	40 days	22/07/15	16/09/15
Contingency Workshops	35 days	12/08/15	30/09/15
Contingency Workshop 1	35 days	12/08/15	30/09/15
Contingency Workshop 2	35 days	12/08/15	30/09/15
Contingency Workshop 3	35 days	12/08/15	30/09/15
Contingency Workshop 4	35 days	12/08/15	30/09/15

Table 4 Programme Extract

7. Technical Competencies

7.1. HAZID Attendance

7.1.1. The technical competency required for each HAZID review exercise will vary depending on the facility area and complexity. Whilst trying to keep the number of workshop attendees between 6 and 12, in general the following areas should be represented as necessary. Some competency areas apart from HAZID Chair and Secretary may be covered by a single representative.

i. Reference Design document lead

ii. HAZID Chair

iii. HAZID secretary

iv. RSSB safety specialists, as appropriate

v. RSSB New Systems representatives, as appropriate

vi. Human Factors

vii. Programme level representatives (both technical system and operations expertise)

viii. Project level representatives, e.g. Great Western

ix. Driver representative, as appropriate

x. Signaller representative, as appropriate

xi. Station staff representative, as appropriate

xii. Maintenance staff representative, as appropriate

xiii. Freight operator, as appropriate

xiv. Passenger operator, as appropriate.

8. Bid Evaluation

8.1. Evaluation Criteria

8.1.1. Bids will be evaluated, and the successful supplier selected, based on a series of weighted evaluation criteria. These criteria are used directly to evaluate the supplier's ability to achieve the project deliverables.

8.1.2. The supplier will fully complete the Evaluation Criteria table, as detailed in Section C – Specification of the Invitation to Tender (RSSB1930ITT), and include it in their bid.

8.1.3. The successful supplier will be able to demonstrate:

i. Experience of delivering similar projects involving UK Mainline Railway HAZID leadership and risk assessment

ii. Experience of delivering similar projects involving ETCS HAZID leadership and risk assessment

iii. Qualification experience and breakdown of resource to deliver the project

iv. Experience of delivering projects that include wide ranging stakeholder engagement

v. Understanding of the current issues and practices and undertake research as necessary

vi. An understanding of the requirements of the remit and appropriate implementation.

8.1.4. Suppliers are requested to provide three references in the PQQ form (attached) of past similar projects from the past three years.

8.1.5. The work is divided into 4 work packages as detailed in Section 4. Table 2: Facilities Subject to HAZID and may be awarded to 2 or more suppliers to ensure that the project is delivered by 30 September 2015. Suppliers are invited to bid for all 4 work packages. However, tenderers are not required to bid for all 4 work packages in order for their bid to be considered. Tenderers should be aware that RSSB will not award all 4 lots to the same supplier.

9. Abbreviations & Definitions

Acronym / Term	Description
ALARP	As Low As is Reasonably Practical
Assigned measures	Mitigating measures that have been assigned to an identified hazard.
CSM for REA	Common Safety Method on Risk Evaluation and Assessment
EDT	(National) ETCS Development Team
ERTMS	European Rail Traffic Management System
ESG	(EDT) ETCS Steering Group
ETCS	European Train Control System
ETCS System Definition	A definition of the ETCS, including operating arrangements, rules, etc.
FMEA	Failure Mode & Effect Analysis
Hazard	A condition, event, or circumstance that could lead to or contribute to an unplanned or undesirable event.
Hazard Analysis	An analysis or identification of the hazards which could occur at each step in the process, and a description and implementation of the measures to be taken for their control
HAZID	Hazard Identification Workshop
OSG	(EDT) Operations Strategy Group

9.1.1. See also the Glossary in the ERTMS Concept of Operations

10. Appendix A

10.1. Related Documents

10.1.1. The following documents accompany this Invitation to Tender (RSSB1930ITT),:

- ERTMS Concept of Operations

10.2. Reference Designs

- Facility JJ Level Crossing Management
- Facility R - Boundaries
- Facility AA Consistent provision of lineside signage
- Facility CC Use of Packet 44
- Facility II Balise Rules
- Facility HH Train Maintenance Facilities
- Facility KK- Transmission of National Values
- Facility LL Track Conditions
- Facility S5 Route Not Proved
- Facility U System controls for issue of Movement Authorities (Route Proving)
- Facility Y – Gradient and Speed Profiles
- Facility Z2 Control of DMI Units

10.3. Templates

- Template for the HAZID Input form (with a macro to create Word records for the report)
- Template for the HAZID Report