Infrastructure Projects

IP W&W
System Safety Briefing
Common Safety Method – Risk Evaluation and Assessment

Sponsors and Project Managers

Ver 0.5 11/6/14
Introductions

• Introductions

• Please complete attendance sheet
Agenda

• Background and Overview
  – Railway legislation
  – Overview of CSM-RA process

• System Safety Concepts

• What does CSM-RA require and when
  – Key documents
  – Aligning with GRIP

• Key Messages
You should understand:

- What CSM-RA is
- What is the background and context
- What is required of Sponsors and Project Managers
- What’s required at GRIP stages
What is the background

• The Common Safety Method for **Risk Evaluation and Assessment** (CSM) came into force on 1 July 2012 to facilitate mutual recognition between Member States of risk evaluation and assessment processes.

• Applies to technical, operational and organisational changes.

• A NR Project Advice Note (PAN0081 Issue 2.0) was published in May 2012 providing information on the change. Being revised at present.

• The PAN was considered an interim measure until standards could be updated. The standards moratorium is still in place and so the PAN has been updated to include templates and more guidance.

  – W&W HoE has issued an email in anticipation of the PAN and GRIP being updated.
The Legal Framework Overview

• The HSW Act clearly places responsibility on those who create the risk to manage it.

• All risks do not have to be removed but the law requires duty holders to do everything ‘reasonably practicable’ to protect people from harm.

• This means balancing the level of risk against the measures needed to control the risk in terms of time, money or trouble. Control measures should be adopted unless they are grossly disproportionate to the risk. This judgment is an essential part of the risk assessment process and will be informed by approved codes of practice, published standards and HSE or industry guidance where available.
EU/UK - Rail Legislation

European Union

- Railway Safety Directive 2004/49/EC (amendments apply)
- Common Safety Method on Risk Evaluation and Assessment Regulation (352/2009)
- Technical Specifications for Interoperability (TSIs) Regulation 2001

United Kingdom

- Railway & Other Guided Transport Systems (ROGS) 2006
  - Key Aspects
    - Risk assessments
    - Safety Verification (SV)
    - Cooperation
    - Managing safety critical work
- The Railway Safety (Miscellaneous Provisions) Regulations 1997
  - Key Aspects
    - prevent unauthorised access to the railway infrastructure
    - prevent accidents to workers from moving vehicles
- The Railway Safety Regulations 1999 (RSR 99)
  - Key Aspects
    - An infrastructure manager must not permit the operation of any train without a train protection system

Interoperability Directive 2008/57/EC (amendments apply)

Railways (Interoperability) Law in 2011

Railway Safety (Miscellaneous Provisions) Regulations 1997
- Key Aspects
  - prevent unauthorised access to the railway infrastructure
  - prevent accidents to workers from moving vehicles

Railway Group Standard GE/RT8270

Amended so application of CSM-RA satisfies SV Law in 2012
## Relevant Statutory Provisions

- Example non-exhaustive list that may be applicable to a change during detailed design/ construction/ life-tome operation / decommissioning / dismantling

<table>
<thead>
<tr>
<th>RSP</th>
<th>Typical Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electricity at Work Regulation 1989</td>
<td>Related to system design and use</td>
</tr>
<tr>
<td>Provision and Use of Work Equipment Regulations 1998</td>
<td>Without working on or near live conductors</td>
</tr>
<tr>
<td>Manual Handling Operations Regulations 1992</td>
<td>Identify safe means of installing</td>
</tr>
<tr>
<td>Construction (Design and Management) Regulations 2007</td>
<td>Specific duties : CDM-C, Designer, Principle Contractor, Client</td>
</tr>
<tr>
<td>Control of Lead at Work Regulations 2002</td>
<td>Work on existing structures</td>
</tr>
<tr>
<td>Confined Spaces Regulations 1997</td>
<td>May need to be designed out of the new infrastructure</td>
</tr>
</tbody>
</table>
What is CSM-RA?

Key aspects:

- Significance of change
- Define the system change
- Risk assessment process
  - Iterative
- Manage and Record the process outputs
- Define safety properties of the change
- Justify the safety of the change prior to use

For information only

Frame work from regulation
What’s produced

- Application to W&W SRP for significance test
- System definition
- Project Authorisation Strategy (Interoperability)
- System Safety Plan
- Hazard Management Record (Hazard Log)
- Safety Justification/Case Report
- Assessment Body Safety Assessment Report

Note: All documents are live as the process is iterative.

What does this mean in NR context?
Summary

• Legal Duty to protect people from harm where reasonably practical.

• Understand and Manage Risk
  – CSM-RA provides a process for risk assessment

• Safety Verification satisfied by application of CSM-RA
  – CIP replaced by Assessment Body
System Safety Concepts
The Railway: A System of Systems

- A “system” is defined as a set or group of interacting, interrelated or interdependent elements (including people and operations) or parts that are organized and integrated to form a collective unity or a unified whole to achieve a common objective.

- A “system”, therefore, has implicit as well as explicit definition of boundaries to which the systematic process of hazard identification, hazard analysis and control is applied.

- The system safety concept helps the system designer(s) to model, analyse, gain awareness about, understand and eliminate the hazards, and apply safety measures (controls) to achieve an acceptable level of safety.

- Hence the importance if the System Definition document
Safe by Design and CSM-RA

Define

Legal Duties

Design Risk Evaluation

Hazard Identification

Design

Review and Monitor

Construction

Staged works

Operations

Maintenance

Disposal

System Safe by design
What happened to my new station?
What does CSM-RA require and when

Key Issues

What documents are required
When are these produced and maintained
Iterative process
Key Documents

- Application to NRAP via **DRAM W&W SRP**
  - Does CSM-RA apply to the project: Significance of change?

- System Definition
  - Defines the change include assets, operation and maintenance

- Hazard Record (Hazard Log)
  - Gathers the evidence for the safety story of the project

- System Safety Plan (Plan for application of CSM-RA)
  - What will be done, when and by whom

- Project Safety Justification
  - Tells the safety story of the project

- Independent Assessment Reports
  - Supports the safety story
Application to W&W SRP (NRAP)

Determine the significance of the Change

What railway system changes are being made?

- Technical (ie assets)
- Operational
- Organisational

All changes should be considered

- The change proposer uses **expert judgement** to assess the impact on safety based on 6 criteria
- Document the findings and any assumption
Making Application to NRAP/W&WSRP

• Sponsor makes an application to NRAP to endorse the significance decision (GRIP 1 or 2) and Interoperability
  – NR/L2/RSE/100/02/F01 issue 02

• Each criteria is considered in the NRAP/SRP application form
  Send all application forms to W&W SRP

• If significant need to engage an Assessment Body (AB)
  – Agree assessment plan with AB
### Six CSM Criteria for significance

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure consequence</td>
<td>Credible worst case scenario in the event of a failure for the change</td>
</tr>
<tr>
<td>Novelty used in implementing the change</td>
<td>What’s new to both the railway and the organisation</td>
</tr>
<tr>
<td>Complexity of the change</td>
<td>How certain is the outcome that the system will perform as predicted?</td>
</tr>
<tr>
<td>Monitoring</td>
<td>The inability to monitor the implemented change throughout its life-cycle and make interventions</td>
</tr>
<tr>
<td>Reversibility</td>
<td>The inability to revert to the system before the change (Note can be difficult to achieve)</td>
</tr>
<tr>
<td>Additionality</td>
<td>Consider the totality of a number of changes either recent or proposed in the area.</td>
</tr>
</tbody>
</table>
**System Definition:** Documenting the change

- **The System Definition**
  - *Its purpose is to complement the hazard record by bounding the scope of the hazard identification and risk assessment process and provide sufficient context to facilitate an assessment of the correct application of the process by an independent body (the assessment body).*

- **The System Definition is to be kept updated through the life of the project**
System Description

- **General description**
  - A summary description of the scope of works.

- **Purpose**
  - What will be achievable after the change

- **Functions and Subsystems**
  - structural subsystems including infrastructure (track & structures), OLE, signalling, etc?
  - functional subsystems including operations and maintenance

- **Boundaries and Interfaces**
  - other interacting systems, both physical (i.e. interacting systems) and functional (i.e. functional input and output) interfaces.

- **Environment**
  - People, existing assets, physical, maintenance

- **Assumptions**

Template is included in PAN0081
Example System Definition available
# System Definition
## When and by Whom

<table>
<thead>
<tr>
<th>GRIP Stage</th>
<th>Tasks</th>
<th>Accountable</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Complete initial system definition</td>
<td>Sponsor</td>
</tr>
<tr>
<td>3</td>
<td>Update with selected option</td>
<td>Sponsor</td>
</tr>
<tr>
<td>4</td>
<td>Update option development</td>
<td>Project Manager</td>
</tr>
<tr>
<td>5</td>
<td>Update with detailed design</td>
<td>Project Manager</td>
</tr>
<tr>
<td>6</td>
<td>Update to reflect as built</td>
<td>Project Manager</td>
</tr>
</tbody>
</table>
Hazard Management Keeping track

- A CSM compliant version of a Hazard Record (or Log) template is provided as a hyperlink in PAN0081
- This template is compliant with Network Rail’s corporate risk assessment process
- Guidance on the completion of the template is contained within it
- More general guidance is available in the reference section in PAN0081
Hazard Management
Hazard Log

• Standard Template available and supporting procedure

• Tells the safety story of the life of the project’ and documents ‘where did you challenge the reasoning behind a decision

• Need to consider at risk groups passengers, workforce and members of the public

<table>
<thead>
<tr>
<th>GRIP Stage</th>
<th>Tasks</th>
<th>Accountable</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Complete initial hazard identification for the change</td>
<td>Sponsor</td>
</tr>
<tr>
<td>3</td>
<td>Update with selected option</td>
<td>Sponsor</td>
</tr>
<tr>
<td>4/5/6</td>
<td>Update as required to reflect project development</td>
<td>Project Manager</td>
</tr>
</tbody>
</table>
HAZID to support option selection
What are the significant hazards?

- Reinstating a double track railway from single track
- Increasing line speed and train frequency
- Upgrading a freight only line to mixed traffic
- Providing a grade separated junction
Project Safety Planning

Aspects Projects should consider:

• Details of the project and system;
• Project Safety Organisation;
• Project Safety life-cycle;
• Project Safety Activities;
• Hazard Management and Risk Assessment;
• Human and Environment Factors;
• Issues, Assumptions and Constraints;
• Configuration management;
• Safety Documentation;
• Project Approval Submissions;
• Product Acceptance;
• Reliability, Availability, Maintainability;
• Key Project Milestones.

Guidance in IP W&W System Safety Strategy
# System Safety Plan

## When and by Whom

<table>
<thead>
<tr>
<th>GRIP Stage</th>
<th>Tasks</th>
<th>Accountable</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Complete initial system safety plan</td>
<td>Project Manager</td>
</tr>
<tr>
<td>4/5</td>
<td>Update as required to reflect project development</td>
<td>Project Manager</td>
</tr>
</tbody>
</table>
Justifying Safety: Safety Case/ Hazard Log Report

• Document Hazard Closure
  – Verifying safety requirements have been implemented
  – Producing a document that demonstrates and justifies that the risks associated with the change have been reduced SFAIRP (Acceptance Criteria) ie enough has been done to reduce risk

• Used by Assessment Body

• Interim reports may be required to support GRIP stages
  – Document in safety plan

• PM accountable

• DPE responsible
### Safety Justification

*When and by Whom*

- Provides the document that tells the safety story from the hazard log
- Provided to Assessment Body (as per safety plan)

<table>
<thead>
<tr>
<th>GRIP Stage</th>
<th>Tasks</th>
<th>Accountable</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Justify risk assessment, safety measures and safety requirements for option selected</td>
<td>Project Manager</td>
</tr>
<tr>
<td>4</td>
<td>Demonstrate safety requirements have been meet in outline design</td>
<td>Project Manager</td>
</tr>
<tr>
<td>5</td>
<td>Demonstrate safety requirements have been meet in detailed design</td>
<td>Project Manager</td>
</tr>
<tr>
<td>6</td>
<td>Demonstrate safety requirements have been meet</td>
<td>Project Manager</td>
</tr>
</tbody>
</table>
Interoperability Authorisation Strategy

• Need to understand scope of change
  – System definition

• Define what TSI apply as a result of the changes?
  – Infrastructure
  – Energy
  – CCS
  – PRM
  – SRT

• Method of assessment

• Required GRIP 3 (PM accountable)
Interoperability (simplified) When and by Whom

NoBo provides conformity check

<table>
<thead>
<tr>
<th>GRIP</th>
<th>Tasks</th>
<th>Accountable</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Define TSIs applicable to change in system definition</td>
<td>Sponsor</td>
</tr>
<tr>
<td>3/4</td>
<td>complete TSI <em>compliance templates</em> appropriate to scope of change</td>
<td>Project Manager</td>
</tr>
<tr>
<td>5</td>
<td>Provide design details to NoBo</td>
<td>Project Manager</td>
</tr>
<tr>
<td>6</td>
<td>Provide production details and <strong>Assessment Body report</strong> to NoBo</td>
<td>Project Manager</td>
</tr>
<tr>
<td>6</td>
<td>Certificate of verification</td>
<td>NoBo</td>
</tr>
<tr>
<td>6</td>
<td>Statement of Conformity</td>
<td>NR</td>
</tr>
<tr>
<td>7</td>
<td>Authorisation for Placing into Service</td>
<td>ORR</td>
</tr>
</tbody>
</table>
Independent Assessment

• CSM requires Independent Assessment Body for * Significant* changes.

• What is the Assessment Body looking for?

• “The Assessment Body checks that the CSM has been followed and also checks the results of the assessment”, including:
  – the definition of the system that is being changed is adequate
  – process for hazard identification was robust and complete
  – the classification of hazards is justified
  – the 3 risk acceptance principles have been adequately applied
  – the hazard log contains the right information about the hazards, associated safety measures, and responsibilities
  – hazards and the safety measures are closed and validated
Assessment Plan

- Agree what’s to be assessed by the AB and when
  - Supported by the System Safety Plan
- Complete by end of GRIP 3 (PM accountable)
- Forms basis of contract with AB
Assessment Report

• Provided by the Assessment Body

• Interim reports GRIP 3,4,5
  – Support stage gates

• Final Assessment Report GRIP 6
  – Supports EiS/Commissioning
## Summary Mapping to GRIP

| GRIP 2 & 3 (Feasibility study & Option Selection) | Determine if change significant (Sponsor)  
|                                                | Sponsor to apply to NRAP to endorse change decision (use form)  
|                                                | Engage with Assessment Body (AB)  
|                                                | Produce System Definition  
|                                                | Produce Safety Plan and Interoperability Authorisation Strategy  
|                                                | Develop Initial Project Hazard Log  
|                                                | Risk assessment of option selection and development (ref in Hazard Log)  
| GRIP 4 & 5 (Single Option Development & Detailed Design) | Continue to develop and review PHL risk assessments during design stages  
|                                                | Record significant design options and decisions (ref in Hazard Log)  
|                                                | Produce interim AB Safety Assessment Report (if required)  
| GRIP 6 (Construction, Test and Commissioning) | Ensure transfer of residual Hazards to appropriate owners complete  
|                                                | Close out Project Hazard Log  
|                                                | Produce Safety Case or Safety Justification Report  
|                                                | AB produces Safety Assessment Report  
|                                                | Produce Project Health and Safety file  
| GRIP 7(Scheme Handback) | Handover safety documents from the project team to the infrastructure operator and maintainer (Route)  

Detailed in PAN0081
Key Message

• Both Sponsors and Project Managers have accountabilities to ensure CSM-RA is undertaken successfully and efficiently, ie right documents and right time, so that the Safety Story is told throughout the life-cycle of the project

When it goes wrong:

• ORR issued 2 improvement notices for failing to demonstrate adequate risk assessment from inception to delivery

• Assessment Body prevented a project from commissioning due to inadequate application of CSM-RA
Call a friend in W&W

- System Safety  John Blowfield
- CSM-RA        Gary Davidson
- Interoperability  Anthony Battrum
- RAM           Paul Barnes
- Assurance     Zoe Dixon
- Track         Sean Murray
- Civils        Paul Townsend
- Telecoms      Trevor Gent
- E&P           Rob Stacey
- Signalling    Andy Free
Training

• CSM-RA course (1/2 day)
  – Invited to attend September/October/November

• Interoperability course (1 day)
  – Can arrange when required (liaise with Anthony Battrum)
Information Sources

- System Engineering Team / System safety
  http://oc.hiav.networkrail.co.uk/routes/ww/Engineering/SystemSafety/default.aspx

- NR Health and Safety Management System
  http://hsms/

- Safety Central
  http://www.safety.networkrail.co.uk/Safety-Groups/Safe-by-Design

- HSE Web site
  http://www.hse.gov.uk/

- ORR
  http://orr.gov.uk/