IET Railway Safety Assurance: The Application and Effect of Common Safety Methods

Charles Stewart
Principal Consultant
Systems and Safety Engineering
20 March 2013
Application of CSM REA

- Understanding how Common Safety Methods for Risk Evaluation and Assessment (CSM REA) will be applied
  - How does CSM REA fit with other legal obligations for safety?
  - Do I have to follow it?
  - What do I need to do?
  - Is this all I need to do?
  - How does it differ from what I do today?
  - What are the key differences I need to be aware of?

- Understanding the vision for success
  - Key points
Application of CSM REA – Where does CSM fit in?

- Railway Safety Directive
- Railways & Other Guided Transport Systems (ROGS) Regulations
- Health & Safety at Work Act
- Common Safety Method on Risk Evaluation and Assessment Regulation
- Railway Safety Regulations
- Interoperability Directive
- Railways (Interoperability) Regulations
- Construction (Design and Management) (CDM) Regulations
Application of CSM REA: Does it apply to me?

- There are exemptions
  - Metros, trams, light rail
  - Networks separate to mainline, private freight infrastructure
  - Heritage vehicles / railways
- Applies to all technical, operational and organisational changes
  - Development of a new train
  - Upgrade of a new train
  - ‘Greenfield’ railway development
  - Resignalling
  - Maintenance renewal
  - Company reorganisation
  - Change in operational processes…
Application of CSM REA: What do I have to do?

1. Significance of the change
2. System Definition
3. Hazard Identification & Classification
4. Risk Analysis and Evaluation
   • Codes of Practice
   • Similar Reference System(s)
   • Explicit Risk Estimation
5. Hazard Management & Records
6. Compliance with Safety Requirements
7. Independent Assessment
Application of CSM REA: Yes, but what happens in the real world?

• Looks like a linear process but it’s not for complex changes:
  • Need to map CSM framework to project lifecycle
  • At each lifecycle stage:
    • What activities need to be done (increasing design definition)?
    • What activities need to be revisited?
    • Who undertakes?
    • Who needs to be involved?
    • How is change to system definition managed?
    • What level of independent assessment is required?
• Complex changes may include both significant and non-significant elements
Application of CSM on REA: Is that all I need to do?

- CSM REA focuses on Risk Assessment
- Engineering Safety Management is broader in scope
  - Organisational principles – safety responsibility, safety culture, etc.
  - Configuration management
  - Supplier management
  - Competence
  - Safety planning
  - Records
  - Risk monitoring
- How CSM REA is applied will need to be included within the Safety Management System
Application of CSM REA: What are the differences from ‘Yellow Book’ for risk assessment?

- Legal Obligation
- Terminology
- Significance Decision
- HAZID irrespective of Risk Acceptance Principle Applied
- Risk Assessment Criteria for Technical Systems (RAC-TS)
Application of CSM REA: What’s the difference in terminology?

- Broadly Acceptable
  - Not same as ALARP framework definition - more akin to ‘negligible’
- Safety measures
  - Options for safety controls and mitigations
- Safety requirements
  - Selected safety measures
- Proposer
  - Responsible for application of CSM REA
- Assessment Body (AB / AsBo)
  - Responsible for Independent Assessment
- Hazard Record
  - Broadly the same as a Hazard Log
Application of CSM on REA: What’s significant?

- Significance decision – first stage of CSM REA applies to all changes
- Two questions
  - Is change safety related?
  - Is change significant?
    - consider 6 specified criteria to determine
    - ORR guidance helps
- CSM REA applies in full for safety related significant change
- Otherwise follow Safety Management System
Application of CSM REA: Does the ‘significance decision’ matter?

• No independent assessment of significance decision, but need to satisfy ourselves
• Must be justified and documented
• May be audited by the ORR
• If we get this wrong:
  • If decided ‘not significant’
    • Change may not be thoroughly risk assessed
    • But depends on what process is applied for ‘non-significant’ change
  • If decided ‘significant’
    • Change may be unnecessarily risk assessed in too much detail
Application of CSM REA: How is CSM REA in full different to what I do today?

- Traditional approach
  - Apply standards and product accepted equipment
    - Identify any novel aspect of change that falls outside of standards
    - Perform HAZID on novel aspects
    - Identify any additional controls / mitigations to be applied
    - No HAZID of non-novel aspects
Application of CSM REA: How does this change what I do?

- For significant changes CSM REA requires HAZID up front
  - Even if intention is to apply standards
  - Need to identify all hazards associated with change
  - For each hazard need to identify one or more risk acceptance principles to apply to control the hazard
  - Risk assessment should be proportionate to the risk being assessed
    - Need to focus on novel hazards
    - Need to show all hazards adequately controlled
Application of CSM REA: What are the implications for applications of standards?

- Standards don’t tend to explicitly identify hazards
- Early adopters may need to develop standard checklists of hazards
- Need to agree whether standard fully controls a hazard
  - Between disciplines (e.g. Signalling and Track)
  - Between stakeholders (e.g. IM and RU)
- Need to determine whether standard satisfies requirement to be a Code of Practice
- Need to consider how to introduce new standards or changes to standards
- Need to apply Similar Reference Systems or Explicit Risk Assessment Principle where hazard not fully controlled (including derogations)
Application of CSM REA: How do I decide whether risk is acceptable (in the UK)?

- Codes of Practice
  - Agreement that Codes of Practice adequately control hazards
- Similar Reference Systems
  - Agreement that imported safety requirements adequately control hazards
  - Providing that basis of original risk assessment adequately addresses our risk acceptance criterion (Tolerable and ALARP or at least broadly acceptable)
- Explicit Risk Estimation
  - Tolerable and ALARP or at least broadly acceptable
  - Or satisfies RAC-TS (Functional failure rate $\leq 10^{-9}$ per operating hour for failures with potential catastrophic consequences)
Application of CSM REA: What if Interoperability Regulations do apply?

- If infrastructure change is ‘major’ then interoperability applies as well as CSM REA
- If Interoperability applies:
  - Application of Technical Specifications for Interoperability (TSI) is sufficient to control hazards associated with applicable systems / interoperable constituents
  - Application of National Notified Technical Rules (NNTR) is sufficient to control hazards associated with specified open points / member state specific cases / derogations
  - Further consideration / application of CSM REA necessary for:
    - System integration
    - Systems not covered by TSI / non-interoperable constituents
Application of CSM REA: The vision for success

- Understand CSM REA and its context
- Determine how to apply in your organisation
- Plan specific activities required for new projects
- Develop a clear system definition with well defined boundaries and refine throughout the project life
- Derive generic mapping between standards and hazards
- Ensure focus is on novel hazards / risks
Any questions?
For more information, please contact:

Charles Stewart  
Principal Consultant  

Lloyd’s Register Rail Limited  
Edward Lloyd House  
8 Pinnacle Way, Pride Park  
Derby, DE24 8ZS  

T  +44 (0)1332 268700  
E  charles.stewart@lr.org  
w  www.lr.org/sectors/Rail