Safety Acceptance for Whole-Railway Projects

Understanding the real safety acceptance challenge

Name: Nick Holmes-Mackie
Title: Sector Head for Transport
Email: nick.holmes-mackie@era.co.uk
Risk Contribution through design lifecycle

Concept Requirement (inc Con Ops)

System Requirements

Subsystem Requirements

Detailed Design

Unit Test

Build

Subsystem V&V

System Integration and Test

System Validation
Design Lifecycle and approvals

Concept and Feasibility
- Acceptance in Principle

Requirements Definition
- Acceptance to Proceed

Design
- Acceptance of Design

Build
- Acceptance for Testing

Install and Commission
- Acceptance for Operation
- Acceptance for Revenue Operation

Operation
Generic Approvals Mechanisms

- Design Approval
- Approval to Test
- Approval for limited operations
- Approval for Revenue Ops

Project Approvals Milestones

- ISA Report
- Safety Case
- ISA Report
- ISA Report
- ISA Report
- ISA Report

Independent Safety Assessment
- Expert Opinion

Railway-level Safety Management
- Information collation, analysis and reporting

Systems Delivery
- Information flows from constituent projects

Safety Data

Safety Requirements

Safety Integration Plan

Design Approval

Approval to Test

Approval for limited operations

Approval for Revenue Ops
Changing Safety Focus through the Development Lifecycle

- Assurance of Operations and Maintenance
- Assurance of Temporary Operational Safeguards
- Build Assurance
- Design Assurance
- Assurance of Plans

Approval of Design
Approval to Test
Approval for limited Operations
Approval for Revenue Operations
Differing focusses of Safety Management

The Key Question: Why do you think that what you have done/are planning to do is acceptable?
How Safety Requirements should be managed

RAILWAY Hazards and Safety Requirements

Operational Safety Requirements

Interface Hazard Analysis

ADCs

Subsystem 1
Safety Requirements (e.g. Signalling)

ADCs
Assumptions
Dependencies
Caveats

Safety Requirements
(shared with Subsystem 2)

Safety Requirements
(shared with Subsystem 3)

Safety Requirements
(shared with Subsystem 1)
Design Lifecycle and approvals

- Concept and Feasibility
  - Acceptance in Principle

- Requirements Definition
  - Acceptance to Proceed

- Design
  - Acceptance of Design

- Build
  - Acceptance for Testing

- Install and Commission
  - Acceptance for Operation
  - Acceptance for Revenue Operation

- Operation
Acceptance in Principle

Is definition of the change provided as basis for planning and initial risk assessment acceptable?

Are the requirements adequately defined and expressed?

Is planning for assurance associated with this change acceptable?

Is the level of safety risk anticipated from this change acceptable?
Acceptance of Design

- Does the design implement the requirements?
- Is the design properly base-lined?
- Are safety and hazard analyses and risk assessment acceptable?
- Are interfacing aspects adequately addressed by the design?
- Is residual risk associated with the design is acceptable? Are operational and maintenance mitigations adequately expressed?
- Have previous comments (if any) been satisfactorily addressed?
Acceptance for Test

Has the asset has been built as designed, installed correctly and subjected to adequate controls to confirm this?

Has adequate test planning been carried out? Is safety risk associated with testing adequately controlled?

Are preparations to operate and maintain this asset under test conditions adequate?

Is risk associated with testing acceptable?

Is risk to existing operations acceptable?
Acceptance of Asset

Has the asset testing programme been successful?

Is the asset, following test, ready for operation?

Is the organisation ready in all respects to manage residual risk through operational controls?

Are arrangements in place to maintain the asset in safe operational order?
Introduction

Definition of System

Quality Management Report

Safety Management Report

• Introduction
• Roles and Responsibilities
• Safety Lifecycle
• Safety Analysis
• Safety Requirements
• Safety Standards
• Safety Audit and Assessment
• Supplier Management
• Safety Controls
• Configuration Management
• Project Safety Training

Technical Safety Report

• Introduction
• Assurance of Correct Functional Operation
• Effects of Faults
• Operation with External Influences
• Safety-related Application Conditions
• Safety Qualification Tests
• Other Outstanding Safety Issues

Related Safety Cases

Conclusions

The real question:
Why will this system be adequately safe in Operation?
Thank you for your kind attention

Name: Nick Holmes-Mackie
Title: Sector Head for Transport
Email: nick.holmes-mackie@era.co.uk