Technical Forum
System Safety and Independent Safety Assessment
Asset Standards Authority
30 April 2015
Scope

- Housekeeping
- ASA purpose and organisation
- Work priorities and progress
- Our future
Housekeeping

• Facilities, amenities & first aid – toilets are on Level 8
• Please do NOT plug in portable electronic devices without prior tagging and testing
• Non Smoking offices
• Emergency exit points – stairwell in foyer
• Assembly point – corner of Help and Railway Streets
Emergency evacuation
Emergency evacuation

Figure 9 - Main fire evacuation assembly area
Technical forums - why are we all here?

• ASA Technical Forums –
  • collaborative sessions
  • share knowledge / experience sharing
  • grow the technical capability of Industry and Transport
  • not conferences or training/development events

• Participate and contribute – we need input and feedback

• Consider outcomes and reasoning rather than checklists – be proactive and seek benefits
  • Improve industry performance and overall condition and function of the transport infrastructure asset
Our purpose and organisation
ASA – beyond standards to whole of life assurance

• “Making it clearer and simpler”
  – For Transport Cluster
  – For Supply Chain
• Collaborating and supporting TfNSW to be an informed and efficient asset owner
  – whole of life assurance
  – asset management
  – standards
  – risk based decision making
• Facilitate increased private sector participation and capability
• Transport Values and Customer focus
Providing expertise across all modes
Our work priorities and progress
Principal asset life cycle roles - TfNSW

Asset Standards Authority

Planning
Projects
Services

Plan Acquire Operate / Maintain Dispose

Policy & Regulation
Investment and Configuration Management Gates

Asset Life Cycle

Plan
- Concept
- Specify
- Procurement
- Design
- Build
- Integrate

Acquire

Operate / Maintain
- Operate
- Maintain
- Evolve

Dispose

Investment Gate 0 - Investment Brief
CM Gate 0
- Investment Gate 1 - Strategic Business Case
CM Gate 1
- Investment Gate 3 - Final Business Case
CM Gate 3
- Investment Gate 5
CM Gate 5
- Ongoing CM Gate 6

End of Asset Life Cycle

CCBs
Gates managed through CCBs
- CCBs

Configuration Management and Asset Assurance Committee
Providing TfNSW with assurance

- Engineering decisions
- Obligations to the owner
- Industry service providers
- Deployment of TfNSW protocols
- Enabling O&M efficiencies and effectiveness

TfNSW Asset Life Cycle Model
O&M relationships – guiding and advising

- Contract & asset performance reporting
- Asset assurance reporting
- Asset Maintenance Plan reporting

Transport Planning
- Review

Transport Services
- Monitor

O&Ms
- Deliver

ASA
- Guide & advise

Asset management advice across TfNSW to support specification of asset configuration and in response to asset performance reporting through O&M contracts

- Asset Integrity Report Review
- Asset Maintenance Plan Review
- Surveillance
Authorised Engineering Organisation (AEO)

Maturity ratings summary

[Graph showing maturity ratings for Engineering Management, Competency Management, Configuration Management, Quality Management, and Systems Engineering. The graph compares documented average, deployed average, combined average, and highest average.]
Standards – harmonising and innovating

• Alignment to international standards
• Support co-regulation method and commitment to national approach
• RISSB relationship
  – Board position
  – Method of alignment to classifications (national / state)
  – Joint standards development and National QRA model support
• Rapid Transit (NWRL/SRT) and Light Rail (ALTRAC, Parramatta and Newcastle)
  – PPP contracts state consortia to develop standards set – ASA oversight
  – ASA to publish and manage on behalf of asset owner (TfNSW)
• CRN and ARTC – knowledge sharing and lessons learnt
• Roads and Maritime
  – Maritime – wharf specification knowledge sharing and initial discussions
  – Roads – advice to road projects interfacing with rail corridor
Standards – monitoring popular documents

Top searches and frequently downloaded files

This table summarises what our audience access and search on the ASA website:

<table>
<thead>
<tr>
<th>Category</th>
<th>Oct 14</th>
<th>Nov 14</th>
<th>Dec 14</th>
<th>Jan 15</th>
<th>Feb 15</th>
<th>Mar 15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total of unique page views</td>
<td>38,739</td>
<td>34,914</td>
<td>26,086</td>
<td>29,202</td>
<td>34,458</td>
<td>36,996</td>
</tr>
<tr>
<td>Most frequent word searches carried out by visitors</td>
<td>spc sole, sole spc, railcorp standards, asset standards authority, asa transport</td>
<td>spc sole, sole spc, railcorp standards, asset standards authority, translay</td>
<td>spc sole, sole spc, railcorp standards, asset standards authority, translay</td>
<td>railcorp standards, aso, asa standards, translay</td>
<td>railcorp standards, aso, asa standards, asset standards authority, asa transport, ts</td>
<td></td>
</tr>
<tr>
<td>Most frequently downloaded files</td>
<td>TS TOC 1 SDG 001 ESG 100 SPG 705 TS TOC 2 Electrical Safety SMS Documents</td>
<td>TS TOC 1 ESG 100 SDG 001 TS TOC 2 ESG 100 Electrical Safety SMS Documents</td>
<td>TS TOC 1 ESG 100 SDG 001 TS TOC 2 ESG 100 Electrical Safety SMS Documents</td>
<td>TS TOC 1 ESG 100 SDG 001 TS TOC 2 ESG 100 ESC 210 Electrical Safety SMS Documents</td>
<td>TS TOC 1 ESG 100 SDG 001 TS TOC 2 ESG 100 Electrical Safety SMS Documents</td>
<td>TS TOC 1 ESG 100 SDG 001 TS TOC 2 ESG 100 ESC 210 Electrical Safety SMS Documents</td>
</tr>
</tbody>
</table>

Table 2 - Top searches and file downloads by month

Construction of cable Routes and Signaling Civil Works

Train Operating Conditions Manual – General Instructions

Train Operating Conditions Manual – Division Pages

Circuit Design Standards

Signal Design Principles

Track Geometry and Stability

Asset Standards Authority Purpose, priorities and progress | 22
List of AEOs

All TfNSW standards

All ASA Communications – presentations and forum material

Frequently searched quick links / hot documents
<table>
<thead>
<tr>
<th>Industry engagement - sharing and listening</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Industry briefings</strong></td>
</tr>
<tr>
<td>• Updates, guidance, thought leadership and awareness</td>
</tr>
<tr>
<td>• Two to four per year to 150+</td>
</tr>
<tr>
<td><strong>Industry round tables</strong></td>
</tr>
<tr>
<td>• Discuss and dissect key topics from industry briefings</td>
</tr>
<tr>
<td>• Two to four per year to approx 60+</td>
</tr>
<tr>
<td><strong>Industry seminars</strong></td>
</tr>
<tr>
<td>• Large technical audiences</td>
</tr>
<tr>
<td>• Detailed and application-specific technical learnings and contemporary subject matter</td>
</tr>
<tr>
<td><strong>Technical forums</strong></td>
</tr>
<tr>
<td>• Capture and share knowledge and experience</td>
</tr>
<tr>
<td>• 20-30 attendees tailored to the subject matter</td>
</tr>
</tbody>
</table>
Future focus
Our future – assuring all modes
Questions?
Introduction
System Safety and Independent Safety Assessment

Richard Adams, Manager Safety and Risk Assurance
Objective

- Identify and discuss issues relevant to safety assurance arising as the AEO concept matures
- Gain industry views around System Safety and Independent Safety Assessment
- Provide industry with information around being an Independent Safety Assessment AEO
Agenda

- System Safety and Safe Design – Are they the same thing? – presentation and related activity
- Morning Tea
- Independent Safety Assessment – Where we are and industry’s views – presentation and related activity
- Lunch – informal discussion
- Transport Projects Delivery Office approach to engineering safety and systems assurance in the new AEO world
Participant Introductions

- Who you are and who you represent
- Why did you want to come here today?
- What do you want to get out of the day?
System Safety and Safe Design
Are they the same?

Claire Owens, A/Principal Safety Change Adviser
Background

• Commonly finding at AEO assessments that Safety in Design is being presented
• Is Safe Design and System Safety the same?
Assurance and AEO’s

AEOs are required to assure new or altered assets/systems:

– **RAM** – operable and maintainable
– **Safety** – ensured SFAIRP
– **Fit for purpose**
– **Whole of life cost**
Legislative Duties

Under the Rail Safety (Adoption of National Law) Act 2012 and Work Health and Safety Act 2011, Transport for NSW and Duty Holders have duties so far as is reasonably practicable (SFAIRP) for the safety of the rail network and its operations.
Definitions

**System Safety** is the concurrent application of systems based approach to safety engineering and of a risk management strategy covering the identification and analysis of hazards and the elimination, control or management of those hazards throughout the life cycle of a system or asset.

**Safe Design** is the integration of control measures early in the design process to eliminate or, if this is not reasonable practicable, minimise risks to health and safety throughout the life of the structure being designed.
System Safety

• System Safety Standard for New or Altered Assets TS 20001:2013
• MIL-STD-882E – System Safety
• European Common Safety method (CSM)
• EN 50126/8/9 – guidance on Reliability, Availability, Maintainability and Safety (RAMS)
• IEC 61508 – Functional safety of electrical/electronic programmable electronic safety related systems
• AS 4292 – Rail Safety Management
System Safety

Key Objectives:

• To integrate safety into the design and development of new or altered assets such that the delivered systems are safe SFAIRP

• To deliver documented assurance supported by evidence demonstrating the safety of the delivered system
System Safety in Life Cycle phases

Plan
- assure the key decisions impacting safety made here
- Risk based decision making – decisions justifiable as ensuring safety
- SFAIRP
- assure the specification

Acquire
- assure the safety of the asset
- assure the integration into the network
- Verification and validation
- assure the operational readiness and maintenance arrangements

Operate Maintain Phase
- assurance of modifications in maintenance
- assurance used in line with its safety argument
- Decommissioning and disposal is a change activity in its own right
Design

Plan phase of the life cycle
- Key decisions impacting safety are made in this phase
- Eliminating hazards at the design or planning stage is often easier and cheaper to achieve than making changes later when the hazards become real risks.

Safe design can result in many benefits, including:
- more effective prevention of injury and illness
- improved useability of structures
- improved productivity and reduced costs
- better prediction and management of production and operational costs over the lifecycle of a structure
Work, Health & Safety Legislation

Previous
• Safety in Design (SiD) or Safety by Design process focussed on design for construction and maintenance

Current
• Work Health and Safety Act 2011 WHS

Safe Design
• Codes of practice – Safe Design of structures
• Guide for Safe Design of Plant
• Guide for Manufacturing Safe Plant
Safe Design

• The WHS Act requires the designer of plant, substances or structures to ensure, so far as is reasonably practicable (SFAIRP) that the plant, substance or structure is designed to be without risks to the health and safety of persons who:
  ✓ Construct/ Manufacture/ Assemble
  ✓ Use (including operators, maintainers) for which it was designed
  ✓ Demolish, Decommission, Dismantle or Dispose
  ✓ In the vicinity of a workplace and exposed to the plant or structure or whose health and safety may be affected by an activity related to the plant, substance or structure

• Note: A Person Conducting a Business or Undertaking (PCBU) who alters or modifies a design without consulting the original or subsequent designer will assume the duties of designer
Similarities

- Safe Design And System Safety
- Start at Concept phase
- Scalable according to complexity and risk
- Risk Based decision Making
- Systems approach integrates risk management in the design phases
- Ensure Safe SFAIRP
- Consultation and Stakeholder Engagement
- Information Transfer
- Considers the life cycle
Key Comparisons

System Safety

- System Safety is a through life cycle set of activities. Takes a whole life cycle view to deliver an asset that it is safe to operate and maintain
- Doesn’t stop at design (Plan phase) – iterative hazard identification and hazard analysis throughout the asset life
- Hazard log purely end use focused
- Includes other activities to provide progressive assurance throughout the asset lifecycle – design reviews, V&V, operational readiness, safety argument, independent assurance where risk demands it
- Systems view – integrate into the network
- Includes software and SIL in much greater detail

Safe Design

- Considers the life cycle - how the design will affect the health and safety of those who will interact with the system throughout its life.
- Includes transitional construction/ manufacturing/ installation WHS risks
- Hazard identification and analysis is completed at the end of design – key information is to be provided to those involved in the later stages
- Hazard log has a mix of asset and construction hazards
Mapped against the Asset Life Cycle

System Safety Activities
- Hazard Log
- Controls

Safety Design
- PHA

Driver
- Concept
- Specify
- Procurement
- Design
- Build
- Integrate
- Accept

Plan

Operate / maintain
- Operate Maintain
- Evolve
- Dispose

CM Gate 0
- I Gate 0

CM Gate 1
- I Gate 1

CM Gate 2
- I Gate 2

CM Gate 3
- I Gate 3

CM Gate 4
- I Gate 4

CM Gate 5
- I Gate 5

CM Gate 6
- MP Gate 6

Dispose

Systems Engineering Investigation

Previous operational experience

Hazard Activities
- PHA
- SHA

Hazard Log

Dracas

Asset Standards Authority Purpose, priorities and progress | 45

A4294416
Summary

- TfNSW seeking assured asset
- Assurance is required to address whole of life
- Duty Holders have duties to ensure safety (SFAIRP)
- System Safety is part of Asset Assurance
- Safe Design opens the door to ensure safety SFAIRP but does it address everything for an assured asset?
Exercise Two

Group activity
Workgroup Questions – Part 1

• Can Safe Design support a Safety SFAIRP assured asset?
• What approach would you take to ensure you are managing your WHS obligations, system safety assurance and engineering activities so that there is an efficient, effective integrated process?
• What is your thoughts on a hazard log which contains construction risks?
Workgroup Questions – Part 2

• What approach would you take for these 3 types of assets pictured to ensure the appropriate level of safety assurance?

• Is Safe Design adequate in any of these examples?

• If you apply System Safety to each project do you get value, is there a cost benefit?
Independent Safety Assessment
Where we are and what’s industry’s view?

Richard Adams, Manager Safety and Risk Assurance
Assurance

Assurance is a set of structured and planned activities conducted through the asset life cycle providing progressive justified confidence that objectives are being achieved and that the asset is or will be fit for purpose.
Assurance Layers

- TfNSW
  - 3rd Party Assurance
- Other AEO / Organisations
  - 2nd Party Assurance
- Delivery AEO
  - 1st Party Assurance

Note: Second Party Assurance may be undertaken by the Delivery AEO or a separate / independent AEO or organisation.

- Project and TfNSW audits, reviews, due diligence and acceptance
- Auditing, independent reviews, independent validation, ISA
- Engineering process, assurance process, risk management etc.
What is ISA?

• Institution of Engineering and Technology -
  …the formation of a judgment, separate and independent from any system design, development or operational personnel, that the safety requirements for the system are appropriate and adequate for the planned application and that the system satisfies those safety requirements

• Suggested TfNSW definition –
  The formation of an independent professional opinion of the validity of a safety argument supporting a new or altered asset
Why do we want ISA in NSW?

- To support the asset assurance framework
- To aid the acceptance of assets
- International good practice
  - Required by EN50129 (Signalling and Comms)
  - Mandated under European Common Safety Method for higher risk changes
- More procurements / technologies from elsewhere in the world – commonality of assurance regime
- Assessment of validity of safety argument through lifecycle
What is the intent of ISA?

- Provides an independent professional opinion of the validity of the safety assurance and safety argument
- Supports the acceptance of assets
- Supports progressive assurance
- Additional assurance level for higher risk changes
- Adds confidence to the assurance process
ISA Role and the Lifecycle

AEO Engagement

Specialization and solution definition

May be benefits in ISA Here

Planning & business needs definition

Operational concepts & Metrics: Options, Analysis & Tradeoff feasibility study

Concept, functional Architecture

System level design & physical architecture

Subsystem level design

Unit level design

Procurement, fabrication/manufacturing/construction/installation

System level integration & tests

Subsystem level integration & tests

Unit level tests

Operations & Maintenance changes/upgrades

Operational system acceptance tests

De commission & disposal

 ISA
ISA Documentation

Technical Information

Independent Safety Assessor (ISA) Requirements (Interim)

Version 1.0
Issued Date: 15 May 2014
Effective Date: 15 May 2014

Important Warning

This document is one set of standards developed, safety and specifically for use in the rail network owned or managed by the NSW Government and its agencies. It is not suitable for general products. You must not use or adapt it in any way unless you have the prior written permission of the NSW Government and its agencies.

This document may not be current. Current standards are available for download from the Asset Standards Authority website at www.transport.nsw.gov.au.

© State of NSW through Transport for NSW

Guide

Guide to Independent Safety Assessment

Version 1.0
Issued Date: 15 May 2014
Effective Date: 15 May 2014

Important Warning

This document is one of a set of standards developed specifically for use in the rail network owned or managed by the NSW Government and its agencies. It is not suitable for general products. You must not use or adapt it in any way unless you have the prior written permission of the NSW Government and its agencies.

If this document forms part of a contract with a NSW Government agency, use of this document is subject to the terms of the contract or approval.

This document may not be current. Current standards are available for download from the Asset Standards Authority website at www.transport.nsw.gov.au.

© State of NSW through Transport for NSW
ASA ISA Framework

- ISA may be appointed by Lead AEO or by TfNSW
- Initial Safety Change Assessment mandates ISA for Significant changes
- Less significant changes at AEO’s discretion
- ISA reports at key lifecycle phases – reports to CCB / CMC
Conduct of ISA

- Identify problems early
- Be aware of and minimise program risk
- Risk based approach
- Don’t just consider documents and standards
- Independently consider risks – informs assessment
- Take different view points to the project
  - System view
  - Asset lifecycle view
Independence

- Challenge – Independence versus value add
- Can’t become part of the solution
- Project owns design decisions

By:
- Good reporting of concerns but not suggesting solutions
- Still working closely – understand the assurance process in detail
Competency of ISAs

Technical Skills
- System safety and safety management
- Assessment and auditing skills

Behavioural Skills
- Judgement, decision making, communication reporting

Knowledge
- Engineering / technology domain
- Standards, legislation and regulatory environment
Interfaces and relationships

- ISA / AEO relationship
- ISA / Project /TfNSW relationship
- ISA must develop and maintain respect and trust
  - ISA can benefit all parties in the project
- Understand the project, people and processes
- Assessment location – close relationships must be maintained
- Continual communication
- Proactive assessment, respond effectively to issues
Requirements to be an ISA AEO

Requirements set out in Independent Safety Assessor (ISA) Requirements

AEO Requirements for:

- Standards Management (ENM11)
- Human Factors (SEM 13 & 14)
- System Safety Assurance Requirements (SEM 17-21)
- Competence Management (CPM 1-20)
- Quality Management (QAM1)
- Knowledge Management (QAM2)
- Record Keeping (QAM3)
Key Factors for an ISA AEO

Competence
- Assembling a competent multi-disciplinary team

System safety
- Must be a suitably experienced organisation
- Human Factors is a key contributor to the safety and operability of systems

Quality Management
- Sound ISA can only work with support of sound quality processes
Authorisation of ISA AEOs - update

- First ISA AEO assessment almost complete
- Second assessment in next couple of weeks
- ISAs currently in place on ATP, NWRL (including second Harbour Crossing), NWRL OTS
- Sydney Light Rail – Altrack will be appointing an ISA
Approach to Authorisation

• Take time for ISA organisations to be assessed
• Project authorisations can be applied
• Authorisation of ISAs from outside NSW
• Review and improvement as we go along
Group activity

What is industry’s view of ISA?
Activity

Part 1 – True or False

• Working in your groups discuss each of the ISA statements on your table. Decide whether you believe they are True or False. In doing so think about and record your reasoning.

• Feedback to the group.
Activity

Part 2 – The ISA’s Role

• Use your thinking from Part 1 to think about the following questions. Try and write 3 bullet points in response to each question.
• Feedback to the group.

• What should the ISA’s role be?
• What more could an ISA do to support assured assets?
• How is the role of ISA beneficial to industry?
• Think of the stakeholders in ISA, what may they gain from ISA?