Technical Forum

Independent Safety Assessment

19 June 2014
Richard Adams, Manager Safety and Risk Assurance
Andy Tankard, Principal Manager SQER
Nick Berry, Manager Industry Engagement
Luke Homann, Principal Manager Audit and Authorisation
Objective

• Provide industry with details of ASA’s position on Independent Safety Assessment
• Gain industry input to the development of the Independent Safety Assessment approach
• Provide industry with information around being an Independent Safety Assessment AEO
Agenda

- Introduction and welcome
- ASA Industry Engagement
- Independent Safety Assessment and TfNSW
- Workgroup session
- Becoming an Independent Safety Assessment AEO
- Questions and discussion
- Lunch – informal discussion
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?
Industry Engagement Update
Nick Berry – Manager Industry Engagement
Nick’s Slides

•Nick’s Slides
Independent Safety Assessment and TfNSW
Richard Adams – Manager Safety and Risk Assurance
Assurance and AEOs

• Post 1 July 2013 assets will be supplied or altered by AEOs
• AEOs are required to assure those assets
  – RAM – operable and maintainable
  – Safety – ensured SFAIRP - applicable to ISA
  – Fit for purpose
  – Whole of life cost
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.
AEO Assurance

- AEO to deliver Asset Assurance argument
- System Safety Standard for New or Altered Assets sets framework
- Stakeholder engagement is key to assurance
- Operational readiness – interface to operator / maintainer
- Residual risks – agreement with operator / maintainer
- Operational assurance argument to CMC
- Intermediate stages - CCB
Progressive Assurance

- Gaining increased confidence through lifecycle
- Governance across lifecycle – defining gateways and means of passing
- Managing risks associated with asset acceptance
- Understanding key risks
- Confirms assurance activities are integrated into engineering activities
- Aids development of a demonstrably SFAIRP outcome
Today’s Model - Systems Assurance

Contracted AEO

- Project Management Assurance
- Combined Safety and Engineering Assurance
- Engineer
- Safety Specialist

TfNSW Project Management Assurance

CMC Acceptance

- Supervising Manager
- Chief/Lead
Context – Asset Acceptance
Asset Acceptance

Asset Life Cycle

- Plan: Concept, Feasibility, Procurement
- Acquire: Design, Build, Integrate, Accept
- Operate/Maintain: Operate, Maintain
- Dispose:

Gates 2, 3, 4 managed through CCBs

Configuration Control Board
Asset Acceptance – Configuration Governance

TfNSW Configuration Management Committee (CMC)  ASA Configuration Control Board

Configuration Control Boards

- Transport Projects Division CCB
- North West Rail Link CCB
- Country Trains CCB
- Sydney Trains CCB
- Other transport modes CCBs
The CMC is the asset and safety risk acceptance authority for TfNSW. Acceptance is based on due process and the demonstration of the assurance case by the party responsible for the change.

- Stakeholders consulted
- Operating considerations addressed
- Maintenance considerations addressed
- Demonstration that selected solution is safety SFAIRP
- Technical considerations addressed
- Proposed assurance and governance plan
Asset Acceptance - CCB Concept

The CCB is the asset and safety risk acceptance authority for a project. Acceptance is based on due process and the demonstration of the assurance case by the party responsible for the change.

- Stakeholder issues addressed
- Engineering approvals obtained
- Safety approvals obtained
- Other technical approvals obtained
- Configuration information updated
- Compliance to assurance and governance plan
ISA – the need
The need for ISA

- Through project assurance function to drive the management of asset risks
- To aid CMC in accepting assets
- To support progressive assurance
- Contribute to a good practice assurance regime
ISA – what is it?
What is ISA?

• Institution of Engineering and Technology - …the formation of a judgement, 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
What is ISA?

- International good practice
- Required by EN50129 (Signalling and Comms)
- Mandated under European Common Safety Method for higher risk changes
- Assessment of validity of safety argument through lifecycle
ISA Structure

• Team Activity
• Lead ISA supported by:
  – Engineering disciplines
  – Process and assurance disciplines
• Audit activities
• Assessment activities
• Management and close out of comments
• Reporting
• Provision of advice
• Maintenance of independence
How is ISA done?

- Requires a proactive approach
- Work closely with Lead AEO
- Do not compromise independence
- Identify and document issues
- Auditable trail of close out
- Uses a risk based approach
- Report regularly and feedback to rail authority
- Done well – minimal issues late in the lifecycle
  - Supports no surprises approach
Independence

- Work with Lead AEO
- Seek to understand
- Identify issues clearly
- Does not provide solutions
- Close out of issues is key
- Traceability of issues and close out discussions
ISA – ASA’s framework
ASA ISA Framework

- ISA will be appointed by Lead AEO
- Initial Safety Change Assessment mandates need for Significant changes
- Less significant changes at AEO’s discretion
- ISA reports at key lifecycle phases – reports to CCB / CMC
Workgroup Activity
Workshop Activity

• What are the competences required for Independent Safety Assessment?
• What processes are required to facilitate and implement safety assessment effectively?
• What relationships and key interfaces need to be managed to enable and to undertake Independent Safety Assessment?
• When in the project and asset lifecycle should Independent Safety Assessment be undertaken and when should it intervene / report to provide maximum value?
Becoming an Independent Safety Assessment AEO
Luke Homann – Principal Manager Audit and Authorisation
Richard Adams – Manager Safety and Risk Assurance
ISA and AEO

• ISA is an independent opinion and authorisation is under the remit of the ASA
• Authorisation through same process as AEO and it will be subject to surveillance
• Assessment can be part of initial assessment or as an addition to scope
• Scoping matrix will need at least an “A” in the corresponding discipline in which they aim to perform their ISA tasks as well as an “A” in the ISA discipline line.
• Work authority (activation) through a contract (not by the ASA) defining terms of reference:
  – boundaries
  – responsibilities
  – liabilities
Scenario

I will provide three scenarios:
1. ISA for an individual discipline
2. ISA for multiple disciplines
3. ISA for overarching network systems integrator
Single discipline scenario

<table>
<thead>
<tr>
<th>Disciplines</th>
<th>Engineering</th>
<th>Architecture</th>
<th>Planning</th>
<th>Preparation</th>
<th>Construction</th>
<th>Maintenance</th>
<th>Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electrical</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mechanical</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Civil</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Assurance “A” in the relevant Discipline

Assurance “A” in the ISA Discipline

Additional details regarding any unique aspects of the authorisation
Multiple discipline scenario

<table>
<thead>
<tr>
<th>Discipline</th>
<th>Assurance “A” in the relevant Disciplines</th>
<th>Assurance “A” in the ISA Discipline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engineering</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Additional details regarding any unique aspects of the authorisation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Systems integrator scenario

Assurance “A” in the relevant Disciplines

Assurance “A” in the relevant Systems Engineering Disciplines

Assurance “A” in the ISA Discipline

Additional details regarding any unique aspects of the authorisation
ISA Competencies
Factors influencing ISA Competencies

• ISA is a through lifecycle approach
• Can be applied to specific engineering disciplines
  – Rolling Stock
  – Signalling / Train control systems
  – Systems / railway integration
• Different product / system levels
  – Generic Product
  – Generic Application
  – Specific Application
• ISA activities
  – Audit
  – Assessment
ISA Competencies

• Lead ISA
  – ISA experience (of similar systems)
  – Assurance / engineering experience in high reliability / safety critical industry
  – Communication / negotiating / reporting skills

• Team Competences
  – Relevant engineering disciplines
  – Systems Engineering
  – Assurance activities, eg testing, verification, software assessment, configuration management
  – Audit
  – Assessment
ISA Competencies

Knowledge
- Human Factors
- Architecture
- Software
- Hardware
- Industry Guidance
- RAMS
- Systems development
- Software development
- "Off the Shelf" certification
- Health and Safety
- E.g. Signalling, Interlocking, Rolling Stock, Communications
- Industry practice and lifecycles
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Technical
- Engineering
- Safety & Technical
- Standards
- Domain (Systems & Technology)
- Risk Management
- Safety Planning
- V&V
- ALARP / SFAIRP
- Safety procedures
- SWI
- Planning
- Defining Safety Claims
- Managing interaction
- Collecting evidence
- Verification
- Assessing Safety Cases
- Documenting Findings
- ISA Reports
- Interaction during project reviews
- Resourcing and team building

Behaviour
- Conduct and Character
- General

Understanding
- Assessment & Audit
- Safety & Technical
- Risk Management
- SWI
- Planning
- Defining Safety Claims
- Managing interaction
- Collecting evidence
- Verification
- Assessing Safety Cases
- Documenting Findings
- ISA Reports
- Interaction during project reviews
- Resourcing and team building

ISA Reports
- Interaction during project reviews
- Resourcing and team building

Industry practice and Technology
- Hardware
- Software
- "Off the Shelf" certification
- Health and Safety
- E.g. Signalling, Interlocking, Rolling Stock, Communications
- Industry practice and lifecycles
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

SAFETY & TECHNICAL UNDERSTANDING
- Assessment & Audit
- Safety & Technical
- Risk Management
- SWI
- Planning
- Defining Safety Claims
- Managing interaction
- Collecting evidence
- Verification
- Assessing Safety Cases
- Documenting Findings
- ISA Reports
- Interaction during project reviews
- Resourcing and team building

Conduct and Character
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

ISA REPORTS
- Interaction during project reviews
- Resourcing and team building

SWI
- Planning
- Defining Safety Claims
- Managing interaction
- Collecting evidence
- Verification
- Assessing Safety Cases
- Documenting Findings
- ISA Reports
- Interaction during project reviews
- Resourcing and team building

Resourcing and team building
- Interaction during project reviews
- Resourcing and team building

Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Presentation of Results to all organisational levels
- Trustworthy / Integrity

Trustworthy / Integrity
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Recognising inappropriate influence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Ability to reach judgements
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Health and Safety
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

E.g. Signalling, Interlocking, Rolling Stock, Communications
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Industry practice and lifecycles
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Software practice and Technology
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Industry Guidance
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

“Off the Shelf” certification
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Health and Safety
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Human Factors
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Architecture
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Software
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Hardware
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Risk Assessment
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Risk Management
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

V&V
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Safety Planning
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Requirements Capture
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Safety Case
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Safety Integrity Levels
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Systems & Technology
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Software Development
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

“Off the Shelf” certification
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Health and Safety
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Human Factors
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Engineering
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

ISA Reports
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Interaction during project reviews
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Resourcing and team building
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Presentation of Results to all organisational levels
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Trustworthy / Integrity
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Maintaining Independence
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Recognising inappropriate influence
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

Ability to reach judgements
- Specific techniques / conventions
- Ability to reach judgements
- Recognising inappropriate influence
- Maintaining Independence
- Team lead
- Presentation of Results to all organisational levels
- Trustworthy / Integrity

ISA Competencies

Transport NSW Asset Standards Authority
ISA Requirements
ISA Role and the Lifecycle

• Early lifecycle
  – Key safety decisions
  – Requirements definition

• Design
  – Progressive assurance
  – Assurance influencing design
  – Address any issues or deficiency early to support SFAIRP
  – Minimise risk is non-acceptance later in lifecycle

• Implementation of design

• V&V – aligned with level of risk
  – Not just functional requirements met but integrity requirements are also achieved

• Key role in acceptance process
ISA Requirements

• Utilised IET Guidance
• Addresses
  – Competency Management
  – Capability and development
  – Reporting
  – Assessment and audit conduct
  – Governance
Competency Management

• Management of competence
• Definition of roles and responsibilities
• Maintenance of capability
Capability and Development

- Maintenance of capability
- Planning, execution and follow up processes
- Match skill sets to authorisation and engagements
- Appointment of Lead ISA and teams
Reporting

• Reporting of issues and milestone Assessment Reports
• Documenting comments, findings and providing traceable records of close out
• Status reporting
• Need for consistent categorisation of issues
Assessment and audit conduct

• Lead ISA and planning
• Absence of commercial, financial or other factors to influence judgement
• Focus on specific aspects not adopt a generic approach
• Risk based approach
Governance

• Review and sign off – independent authority in organisation
• Linking specific role to competence
• Maintenance of independence
• Risk related processes – supporting SFAIRP
• Business continuity
ISA - Next Steps

• Guide to ISA and ISA AEO Requirements are now published
• Engaging industry
  – Potential ISA organisations
  – AEOs that may be required to engage ISAs
  – Technical forum (June)
  – Follow-up communications
• Authorisee ISA organisations
Questions / Closing Discussion