Insights

Effective Assurance of Rail Projects

Used in the context of everyday conversation, the term assurance means to provide 'a positive declaration intended to give confidence', according to the Oxford English Dictionary.

However, when used in the context of rail safety, project management or engineering design, the term can take on different meanings. Unfortunately, the existence of multiple, but often related meanings for the word can lead to considerable confusion.

Having worked as an assurance practitioner over the past 20 years, primarily in the rail industry, I have experienced the existence of multiple meanings to be a common source of confusion, both within and between organisations involved in delivering rail projects. This confusion can lead to inefficiencies through duplication of effort, but also gaps and an over-reliance on ineffective assurance activities. At best, the consequence of such confusion is the waste of money. At worst, it is the missed opportunity to prevent highly visible project failure.

Despite the common issues surrounding the term and its application in the rail industry, we will explore the notion that the function of assurance is simply to deliver an evidenced argument that will provide organisations with justified confidence that a project has met its set objectives.

In doing so, we can also argue that assurance achieves the same outcome as systems engineering and therefore can be considered part of the same process.

In addition to examining the close relationship between assurance and systems engineering, this paper will also:

- Explore the various concepts and associated meanings of assurance.
- Identify common themes.
- Explore more precisely the aims and context of assurance in rail projects.
- Suggest questions that will help understand how assurance can be effective.

2. Assurance Concepts

To illustrate the diversity of meaning, Table 1 includes a selection of definitions of assurance which can be found written down. There is even more diversity of meaning if you also consider the use of the term without any definition given.

Table 1: A Selection of Assurance Definitions

Reference	Term	Definition Provided
UK Rail Safety and Standards Board (RSSB) [1]	Assurance	A positive declaration intended to give confidence.
	Supplier Assurance	The generic term for actions, processes and procedures applied by a customer, to ensure effective use of suppliers.
	Safety Assurance	Confidence that risks, behaviours and processes that are potential threats to safety are being managed and controlled to acceptable levels through appropriate measures.
UK National Audit Office [5]	Assurance	An independent assessment of whether the required elements to deliver projects successfully, such as good project management practices and appropriate funding and skills, are in place and operating effectively.
Association of Project Managers [10]	Project Assurance	The process of providing confidence to stakeholders that projects, programmes and portfolios will achieve their scope, time, cost and quality objectives, and realise their benefits.
HB 158—2010 Delivering assurance based on ISO 31000:2009 Risk Management — Principles and guidelines	Assurance	A process that provides a level of confidence that objectives will be achieved within an acceptable level of risk.
ISO/IEC 15026-1:2013 Systems and software engineering — Systems and software assurance [6]	Assurance	Grounds for justified confidence that a claim has been or will be achieved.
	Assurance Case	Reasoned, auditable artefact created that supports the contention that its top-level claim (or set of claims), is satisfied, including systematic argumentation and its underlying evidence and explicit assumptions that support the claim(s).
Transport for London (TfL) Integrated Assurance Framework [7]	Assurance	The means by which a party responsible for a business activity and its stakeholders gain confidence in the appropriateness of the organisation's decision making and the effectiveness of internal controls.

Reference	Term	Definition Provided
Transport for New South Wales (TfNSW) Assets Standards Authority (ASA)	Assurance	An objective examination of evidence for the purpose of providing an independent assessment of risk management, management control or governance processes for an organisation. [8]
		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. [10]
		A positive declaration intended to give confidence. [9]
	Engineering Assurance	The evidence that planned outcomes have been achieved, or the evidence of effective management of risk. [9]
	Systems Assurance	Systems assurance is the planned and systematic set of activities that demonstrate how the systems and products shall conform to requirements for safety, reliability, availability, maintainability, standards, procedures, and regulations. [9]
	Safety Assurance	Demonstration that all safety risks have been assessed and managed/mitigated SFAIRP (So Far As Is Reasonably Practicable) and satisfy the risk tolerability criteria. [8]
North Atlantic Treaty Organisation (NATO) [11]	System Assurance	Justified confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle.
US Air Force Space Command Design Assurance Guide [12]	Design Assurance	Design assurance is a formal, systematic process that augments the design effort and increases the probability of product design conformance to requirements and mission needs. The activity associated with design assurance has, as its objective, a truly independent assessment of the overall process for development of engineering drawings/models/analyses and specifications.

Common Interpretations Within Rail Project Context

Rail Safety Assurance

The UK RSSB is one of the few organisations that has explicitly defined assurance (see Table 1). It describes assurance at three levels: Company (assurance within an organisation), Company to Company (assurance given by one company who exports risks to another company who imports risks), and Railway System (assurance given by the industry to external parties such as government, passengers and the public).

It focuses on the assurance of BAU (Business As Usual) operational safety, rather than the risks and parties involved in a major project.

Otherwise, the term safety assurance in the rail context usually means the activities and process for managing engineering safety encapsulated in such industry standards and guides as EN 50126 [2] and the iESM Handbook [3]. These activities are necessary to fulfil legal duties under the Rail Safety National Law in Australia.

Independent safety assessment, which is the assessment of project safety management activities by an independent party, may also be included in the concept of safety assurance.

Project Assurance

Project assurance relates to the concept of assurance in project management. It is usually performed by parties independent of the project and results are reported to project governance forums (e.g, project boards) external to the project. The level of rigour, effort or importance placed on the assurance activities is dependent on the perceived risk associated with the project. Project assurance tests that the defined control limits for each project are appropriate and highlight whether they have exceeded, or are in danger of exceeding, limits of variance against target time, cost, quality, scope, risk or benefits.

Systems Assurance

The term systems assurance is commonly used in rail projects to cover activities related to one or more of the following: safety, RAM (reliability, availability, maintainability), quality, network/cyber-security, and compliance to standards and regulations. While this term is in common use, it is difficult to locate any authoritative sources of a definition, except for the NSW Assets Standards Authority (as provided in Table 1).

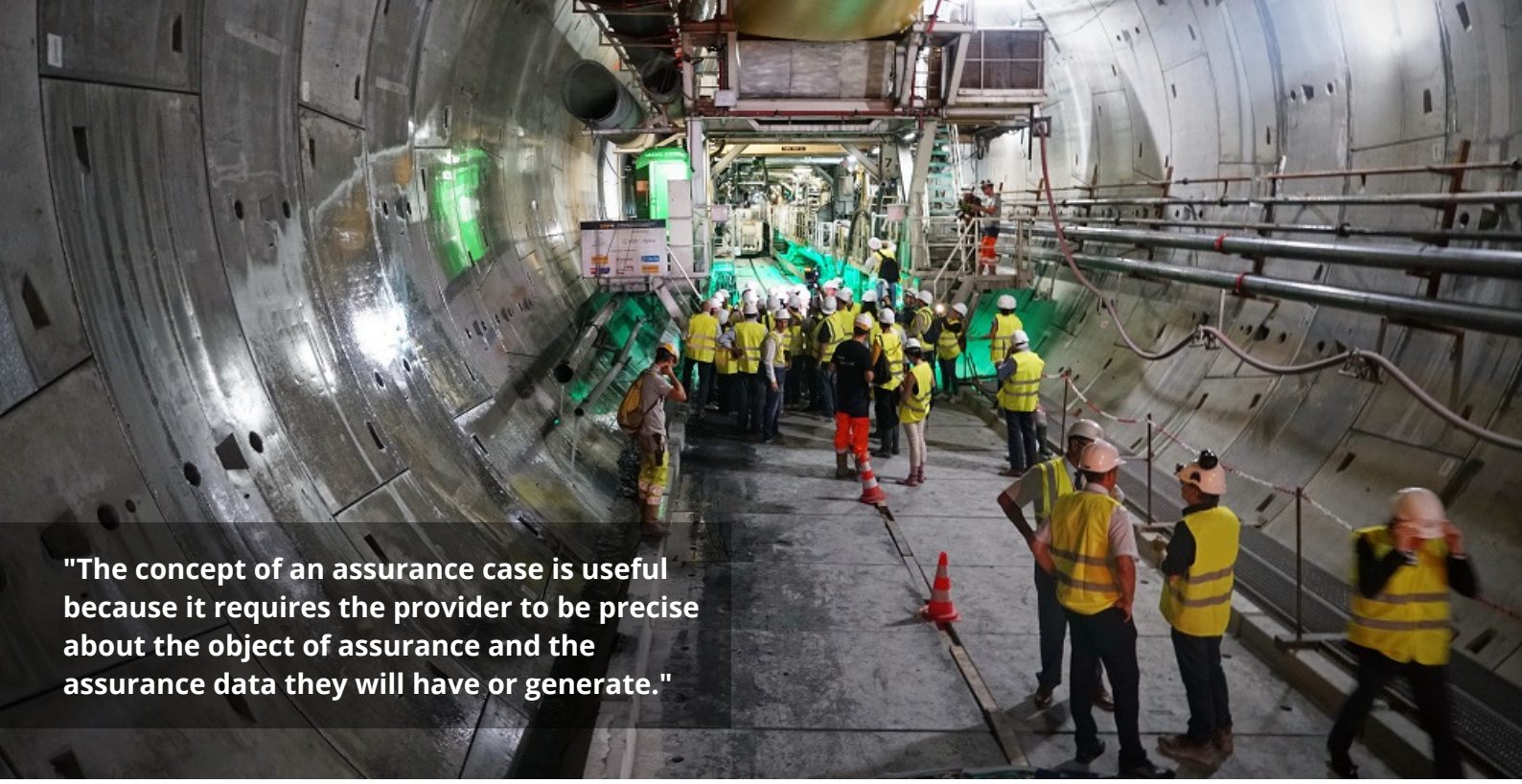
More generally, the standard ISO/IEC 15026 describes the notion of an assurance case as the artefact created to support a claim. The standard states that its scope is assurance for properties of systems and software within life cycle processes for a system or software product. This is a generalisation of safety cases to system properties other than safety and therefore can be considered to apply to other desirable emergent properties of a system, such as safety, reliability, security etc.

Engineering and Design Assurance

The terms engineering assurance and design assurance are usually used to refer to activities (mostly review by a checker) that are executed to confirm that engineering and design outputs meet standards and applicable requirements.

Engineering and design assurance can also be called verification activities, where verification (as per INCOSE Handbook [13]) is a process to provide objective evidence that a system or element fulfils its specified requirements. It may also incorporate some validation activities, such as challenging whether the design will fulfil user, stakeholder or business requirements.

In addition, engineering and design assurance often implies the use of staged gate reviews to establish confidence in a given stage of design or implementation to enable the next stage to progress at a known maturity - for example construction, test or integration readiness reviews.



"The concept of an assurance case is useful because it requires the provider to be precise about the object of assurance and the assurance data they will have or generate."

Common Themes

Despite the lack of consistency in defining the term assurance, there are common themes:

- The positive outcome of assurance is an increased confidence in something – we can call that something the object of assurance.
- It typically involves an assurance provider, who carried out assurance activities, and one or more assurance receivers.
- Assurance often involves some level of independence between parties.
- The assurance receiver determines whether the assurance outcome is positive.
- It can be considered a risk management activity.
- It is implied that the assurance provider generates assurance data as an output of assurance activities.

Assurance Cases

The effectiveness of assurance activities relies on a clear understanding of:

- What is the activity providing increased confidence in?
- What risks is it helping to manage?
- Who are the receivers of the assurance?
- What will the receivers of the assurance do with the assurance data they receive and how will it be determined to be adequate?

The most useful concept of assurance is that from IEC/ISO 15026, which defines an assurance case as a "documented body of evidence that provides a convincing and valid argument that a specified set of critical claims regarding the system being implemented by a project".

Using this concept, we can start to more clearly articulate the object of assurance, what we want confidence in, as one or more claims.

Once a claim is articulated, we can also be clearer about the assurance data we need to generate. We can do this by identifying evidence and developing a structured argument, explaining how the evidence demonstrates that the claim is true.

People often find it useful to map out such arguments in a graphical way. Goal Structuring Notation (GSN) [15] is one well-known way to graphically represent an assurance case, where:

- The claim is represented as a goal **(fig. 1)**.
- The argument consists of a decomposition of

the top-level claim into sub-claims (sub-goals).

- The decomposition is sometimes supported by an explicit strategy.
- When a sub-goal is suitably simple, they are linked to a solution, supporting evidence that provides direct demonstration of the sub-goal.

In summary, the concept of an assurance case is useful because it requires the assurance provider to be precise about the object of assurance (the claim) and the assurance data (argument and evidence) they have or will generate.

It also provides assurance receivers with a structure they can systematically review and assess to determine what elements of the argument they accept or not. Graphical representations can help communicate the assurance case to the assurance receivers.

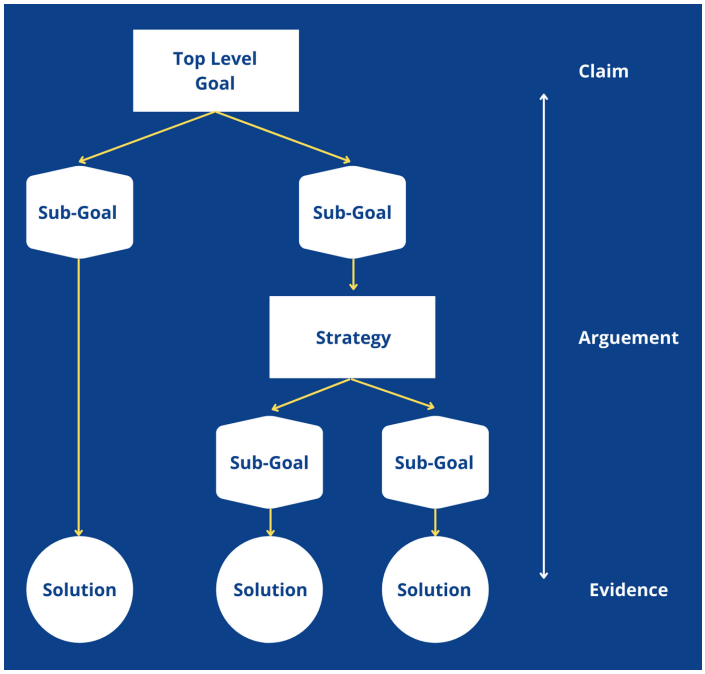


Fig. 1 - Assurance Cases in Goal Structuring Notation

3. Assurance Dimensions of a Rail Project

In simplistic terms, a project makes a change to a railway. Major projects will often deliver a number of interim changes to the railway leading to a final end state which can be considered as transition back to BAU for rail operations (see Figure 2).

It should also be noted that the change to the railway is not just the change to the physical assets, but also to the operational processes and the people involved in running the railway. All of these aspects should be considered part of the railway as a system.

Fig. 2 - Project as a Sequence of Change

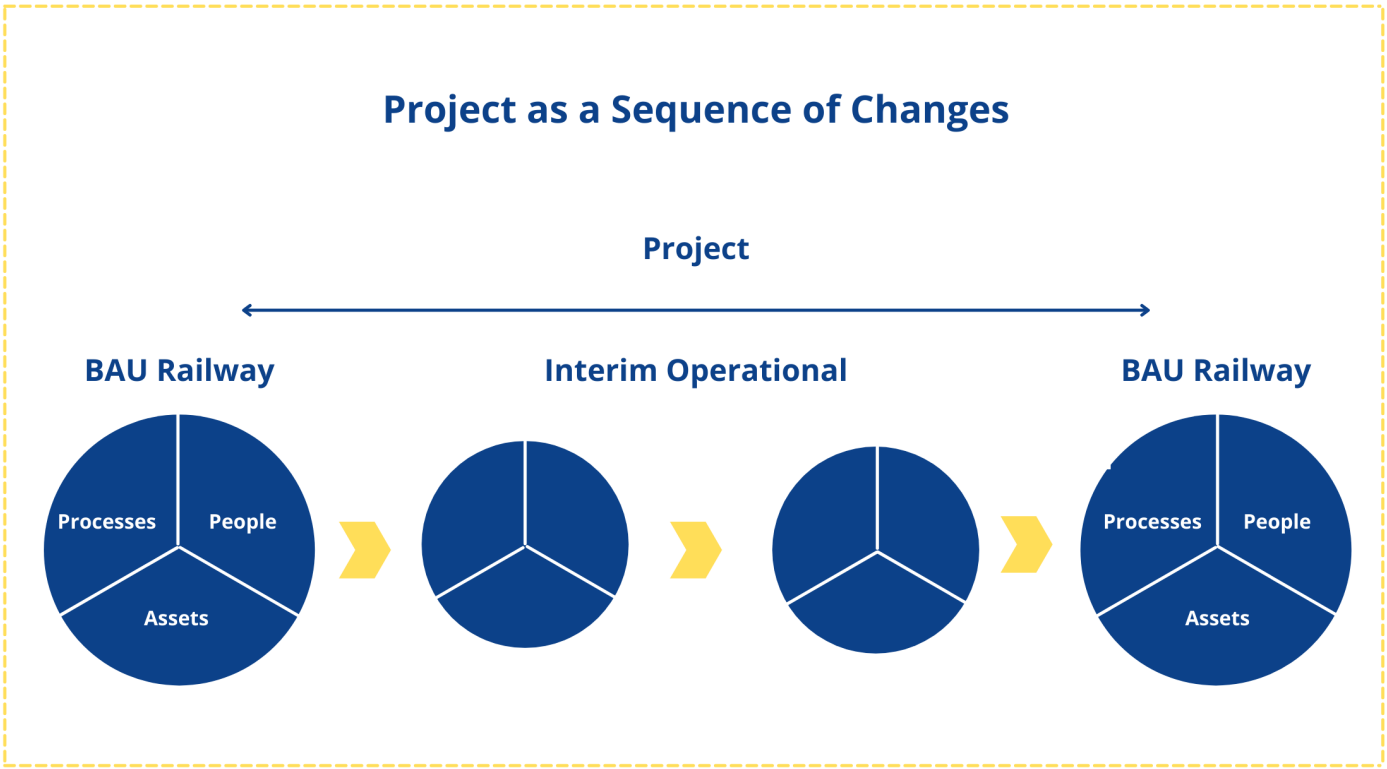
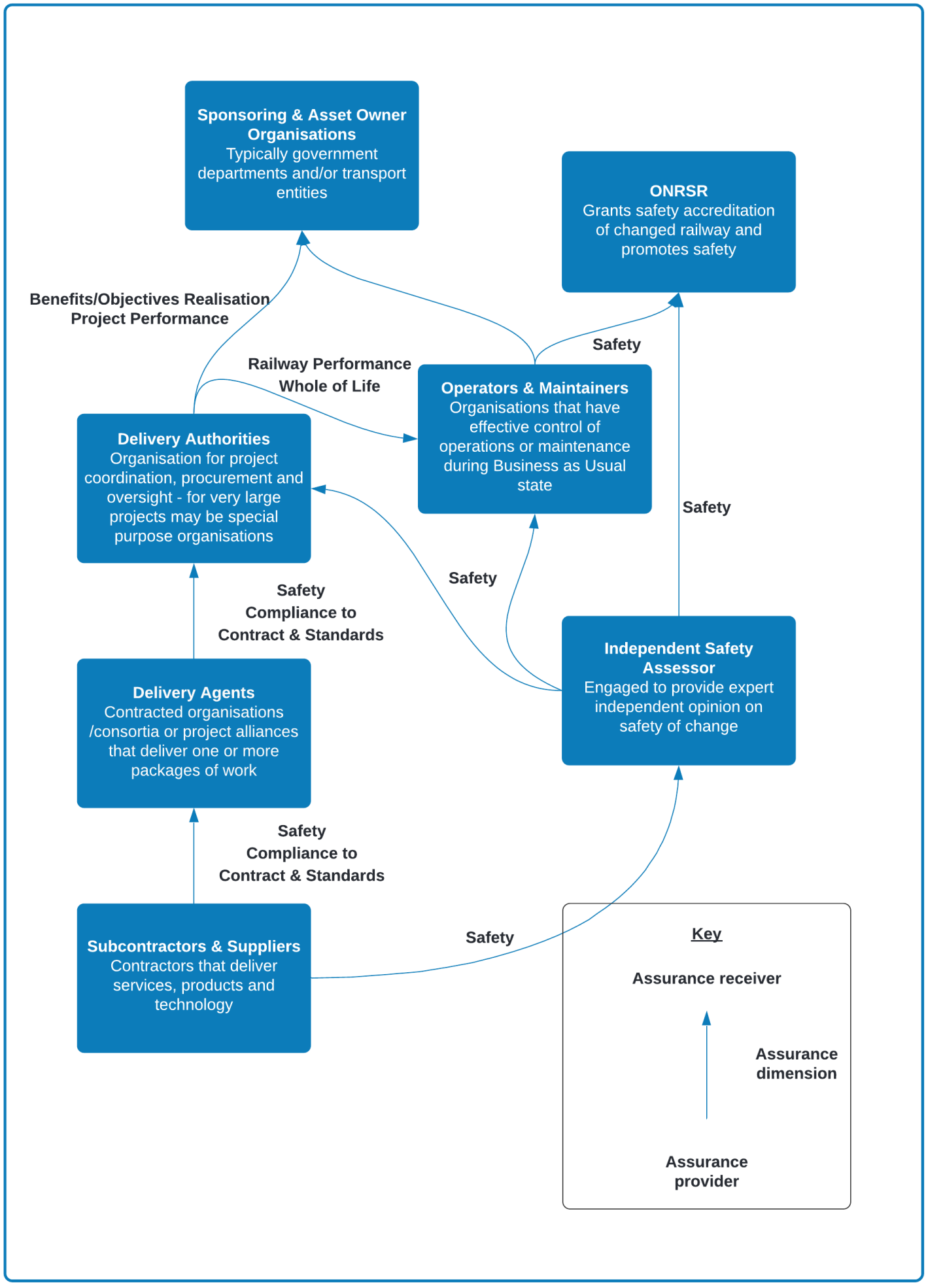


Fig. 3 Providers & Receivers of Assurance in Rail Projects



This view aligns with the regulatory viewpoint of managing safety within a project as managing change to the railway so that operational safety remains acceptably safe. Any assurance activity related to a project can be seen as providing confidence in the product of the project, the changed railway, or in the project itself in terms of how much time or money it will take to effect the change.

Based on the discussion in Section 2, assurance activities can be considered to focus on one or more of the following dimensions:

- Rail safety
- Railway performance, e.g. capacity, journey times, frequency and duration of delays
- Compliance to contract
- Project performance against time or cost
- Compliance to requirements
- Compliance to standards
- Benefits/objectives realisation
- Whole of life considerations.

Figure 3 depicts parties typically involved in a project within the Australian Rail context, and shows which parties typically provide and/or receive assurance. Each project is different, and the exact relationships between parties may be different to what is depicted in Figure 3.

In some cases, the same organisations may fulfil more than one role, and PPP (Public-Private Partnership) project procurement arrangements are likely to be more complex where the delivery agents also take on some role in operations or maintenance and may also have other investors that act as receivers of assurance.

4. Assurance Claims for Rail Projects

For each dimension listed in Section 3, we can now start to more precisely articulate the claims associated with each dimension. We can also articulate the risks as the associated adverse outcomes if the claim turns out not to be true.

From a planning perspective, the claim should be in the future tense about the railway following the implementation of the changes and is articulated in the present tense when the evidence has been provided.

Table 2: Assurance Dimensions and Associated Claims and Risks

Assurance Dimension	Assurance Claims	Managing Risk That
Rail safety	The change will enable the railway safety performance to achieve a target level of safety. All reasonably practicable measures to improve safety will have been taken in the design and implementation of the changes.	The change introduces additional risk or an unacceptable level of risk. Opportunities to improve safety are missed.
Railway Performance	The change will enable specified performance measures of the railway to achieve a target level. For example, performance measures may include the number of delayed services per unit time, or the number of delay minutes, or the number of corrective maintenance actions. Improvements on performance measures may be project benefits/objectives (capacity increase, service frequency increase, journey time decrease). If they are not, there may still be an assurance goal (which should be driven by an explicit requirement) to demonstrate that performance is not worse.	Changes to the railway degrade performance or do not deliver the desired/needed performance benefits.
Project Performance	The project will deliver within agreed variance: • By the planned completion date • Within the budgeted cost • With the defined quality and scope • The benefits identified as part of the business case Note that the last two of these points are covered by Compliance to requirements and Benefits/Objectives Realisation dimensions.	The project delivers late or over-budget.
Compliance to Contract	The contractor will deliver in compliance to the contract.	The contractor does not comply, which in turn is likely to result in the realisation of one or more other risks listed in this column.
Compliance to Requirements	The change will satisfy its specified requirements.	The project does not deliver to the specified requirements, and therefore the project also fails to deliver its expected benefits and objectives.
Compliance to Standards	The implementation of the change and/or the changed railway comply to specified or applicable standards.	Non-compliance to standards which may result in the realisation of other risks listed in this column (such as safety or other performance risks).
Benefits/ Objectives Realisation	The project delivers benefits which justify its cost. The project meets its objectives.	The project costs outweigh the resulting benefits to the railway and subsequently to its investors.
Whole of Life	The change has been designed and implemented to optimise operational and maintenance costs.	Operational and maintenance costs of changed railway are unreasonable (Delivered change is a “white elephant”).

5. The Relationship Between Assurance And Systems Engineering

On closer inspection of the claims listed in Table 2 they can be reduced to a project meeting a suitable set of objectives, including rail safety and other performance objectives for the changed railway; or time and budget.

There is also clearly a significant overlap with systems engineering concepts, in particular, verification and validation. Verification is the confirmation, through the provision of objective evidence, that specified requirements have been fulfilled. Validation is the confirmation, through the prevision of objective evidence, that the requirements for a specific intended use or application have been fulfilled, that a system is able to accomplish its intended use and objectives [13].

Most of the claims can be reduced to the problem of demonstrating that the project will meet a set of objectives for the changed railway. The main task of assurance is therefore to provide an argument and supporting objective evidence that those objectives are met. This is in effect what the effective application of systems engineering principles and processes achieves, and therefore it is possible to consider assurance to largely be one and the same activity as systems engineering.

However, there is a subtle difference in emphasis – assurance has more emphasis on the demonstration to one or more other parties (the receivers of assurance) of objectives. One of the reasons for this emphasis is the underlying legal and regulatory obligations associated with some assurance dimensions. The concept of assurance cases makes this very clear by identifying claims (goals), arguments and evidence as the constituent elements of assurance. Constructing an argument implies there is another party that needs to be convinced the claim is true.

However, there are approaches to systems engineering that also incorporate arguments (satisfaction arguments) [10].

These satisfaction arguments help to justify the correctness of lower-level, more detailed specification derived from higher-level requirements. They provide the explanation why satisfaction of higher-level requirements flows from the satisfaction of lower-level requirements.

Adopting a systems engineering approach that incorporates the development of arguments as part of project processes will provide very effective and efficient assurance as a result.

6. Considerations for Effective Planning

Rail Safety

The activities required to achieve safety claims are relatively well understood and normally documented in a system safety or safety assurance management plan.

The project authority and/or delivery agent should address the rail safety goals through analysis of the safety risk of the proposed changes (assets, processes and people) to the railway, and provide a safety argument and supporting evidence in the form of one or more safety assurance reports or safety cases. They may be required to be an accredited rail transport operator for the design and construction activities of the project.

Under Rail Safety National Law, suppliers and subcontractors also have an obligation as designers, manufacturers, and suppliers, to ensure that rail infrastructure or rolling stock assets are safe for their intended purpose and provide information on the safe use of assets.

The subcontractor/supplier should consider what records and documentation it will maintain in order to demonstrate it fulfilled its obligations. However, any specific requirements for demonstrating safety must be set as part of commercial arrangements.

In addition, ONRSR's expectations and common industry practice is to provide an additional level of confidence through the engagement of an independent safety assessor who will provide an

independent professional opinion of the validity of the safety argument.

Key considerations are:

- Who engages the independent safety assessor to provide maximum level of independence?
- Safety arguments should be developed by those in control of corresponding activities and be scoped accordingly.
- Operations and Maintenance (O&M) organisations must provide input as end users and agree any residual risk they inherit.

Railway Performance

There are many performance factors of relevance to the operation of a railway. Every change to the railway can potentially affect positively or negatively those performance factors. Project objectives and business cases are often focused on significantly improving one or more of those performance factors.

Demonstration of claims related to the performance factors of the railway are quite complex as they usually require sophisticated analysis, such as operational modelling and RAM analysis. There is usually significant complexity in being able to meaningfully connect the performance of the railway at the operational level with the performance of constituent assets. This is rarely done well and often a program of RAM management and engineering activities are executed without clear connection to operational objectives.

There is also often a tendency to include RAM management as part of safety management/ assurance even when there is little relationship between RAM performance of assets and the emergent safety performance of the railway.

Key considerations are:

- What railway performance factors is the project aiming to improve, and what level of improvement does the business case rely on?
- How are those factors measured on the operational railway?
- How can performance requirements on assets be derived from the railway performance requirements? Or how can railway performance be predicted from asset performance?
- How will performance models be used for predictions be validated? What simplifications will need to be made and what is the justification for those simplifications?

Compliance to Contract

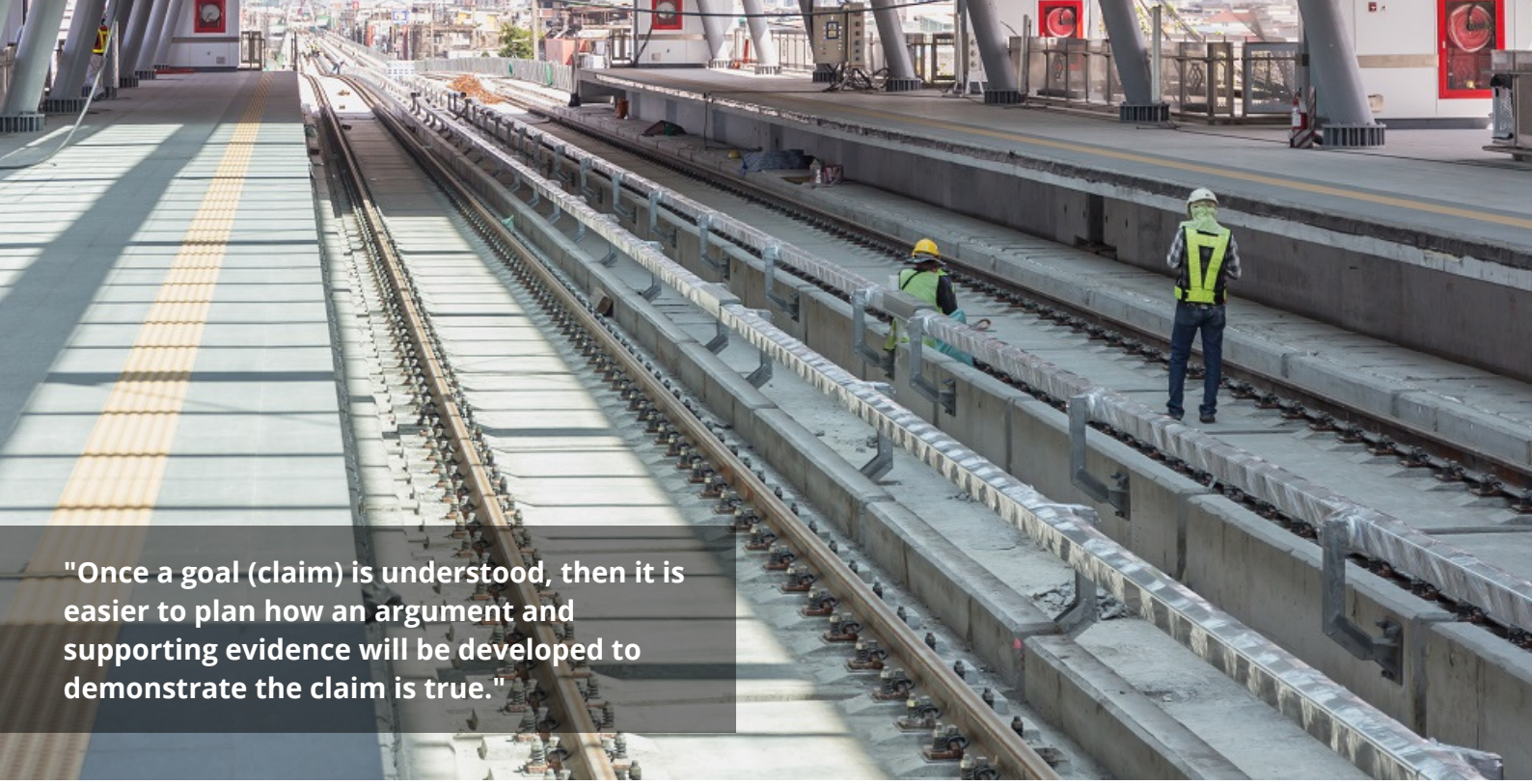
Compliance to contract is only significant for the resulting railway because it shapes what is delivered, and therefore may contribute to the delivery of a change to the railway which does not meet project objectives. Therefore, in addition to any activity that monitors, assesses or certifies compliance to contract, there need to be activities that check that the contract articulates what is required to be delivered to demonstrate (within the contract scope) project objectives, operational safety, performance and whole of life costs.

A contract typically specifies both technical and process requirements. Technical requirements need to be consistent with project requirements so that satisfaction of project requirements follows from compliance to the contract and any non-compliance can be assessed for impact.

Contract process requirements enable the principal to the contract to define minimum standards for required evidence, and to receive documentation and evidence in a format that can be more easily incorporated into wider arguments to satisfy claims. In construction projects, it is common for an independent certifier to ensure both delivery authority and delivery agent meet their obligations under the prime contract.

Project Performance

Project performance is the overall measure of a project against time, cost and quality. This is the essence of project management. As summarised in Section 2, audit processes can provide additional confidence that the project will deliver within its control limits.



Time and cost are easily measured. The measurement of quality then falls back to the other dimensions described here: safety, product performance, compliance, and whole of life considerations.

Compliance to Requirements

While this may be considered an assurance goal, the process of generating evidence of compliance to requirements is central to systems engineering processes and planning the argument and evidence for this goal forms a Verification Plan.

As per INCOSE guidance, compliance to requirements is a two-stage process: verification that design is an agreed-to transformation of requirements and verification that the built system meets the agreed-to requirements, called design verification and system verification respectively.

Note that validation is a different concept, which is the demonstration and generation of objective evidence that the change, once effected, fulfills its objectives and stakeholder requirements.

Compliance to Standards

Compliance to standards is not inherently valuable as a project outcome. It is only useful as a means for demonstrating:

- That well-understood safety and product performance risks are managed through the application of the standard.
- Requirements or contract compliance, where the requirements or contract explicitly call out the standard.

Compliance to standards may be part of the independent certifier's role to review.

Key considerations are:

- How will compliance to standards be demonstrated?
- How will applicability of a standard be determined?
- How will interpretation of standard be validated?

Benefits/Objectives Realisation

The objectives of a project are not to make specific changes to a railway, but to make changes in order to achieve a higher-level outcome e.g. increased capacity, greater convenience for passengers, shorter journey times etc. These are the objectives on which the business case of a project is based.

Benefits realisation management is the term used in project management methodologies to describe the activities that ensure identified benefits are

realised as project implementation progresses. Within the systems engineering discipline, these objectives are commonly analysed to capture business and stakeholder requirements.

Some of these project benefits or objectives may be measurable after delivery in the final BAU operation of the railway. It is relatively straightforward to measure head ways, journey times or similar once the changed railway is in operation.

However, the relationship between the high-level objectives, which are typically emergent properties, and the specific asset and operational changes that are delivered by a project are often not straightforward. Providing confidence that the specified changes (at whatever level of design or implementation abstraction) will deliver the expected outcomes requires significant analysis and argument and an iterative approach in order to effectively deliver. Thinking needs to be conducted contextually and hierarchically.

Interestingly, even though a project's existence is dependent on the correctness of the change specification, little is often done to confirm it progressively. Requirements management activities may include an attempt to provide traceability from lower-level requirements and specifications to business requirements, and the existence of such traceability may be required to support project gateway reviews. However, the traceability is often not supported by any substantial analysis or argument, nor is it subject to significant rigorous review.

Sometimes, some form of technical review, including the engagement of independent peer reviewers, is held at key points to challenge whether the proposed solution and its development is appropriate. But this review is often solely reliant on the expertise of the reviewers and rarely follows a systematic examination.

The explicit use of arguments to support the adequacy of project technical requirements to meet high-level objectives could greatly improve the likelihood project objectives and benefits are met.

Whole of Life Considerations

From an assurance perspective, whole of life considerations are often neglected. Project-focussed organisations (project authorities and delivery agencies) are biased not to focus on these considerations. It therefore becomes important for the O&M organisations to play a key role here both in terms of providing input to the development of requirements and solutions and as the assurance receivers against this dimension.

This can be suitably managed by using current operation and maintenance costs as a measurable baseline. High-level project objectives can aim to constrain O&M costs to only increase proportionate to any increase in number or size of assets. In some cases, one of the project drivers may be to reduce O&M costs. Suitable progressive demonstration requires analysis and the development of an argument in early phases.

7. Conclusion

This paper has shown that while assurance in the context of rail projects can mean many things and many different concepts are often conflated into one, it is possible to be quite precise about the goal or claim for which assurance is provided and received. Once a goal (claim) is understood, then it is easier to plan how an argument and supporting evidence will be developed to demonstrate the goal/claim is true.

The paper also develops an argument that the activities associated with most assurance goals are inherently systems engineering activities. When one adopts an approach to systems engineering that includes an emphasis on providing arguments that project objectives are met, primary assurance needs will be addressed.

Katherine Eastaughffe | Principal Consultant

References

1. UK Rail Safety and Standards Board (RSSB), 2013. Safety Assurance Guidance: Guidance and examples of good practices in safety assurance in Britain's railway industry. London

2. European Committee for Electrotechnical Standardization (CENELEC), 1999. Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety

3. Technical Programme Delivery Ltd, 2013. International Engineering Safety Management (iESM) Handbook – Good Practice Handbook. London

4. Association of Project Managers, 2014. A Guide to Integrated Assurance. Buckinghamshire

5. UK National Audit Office, 2012. Assurance for Major Projects. London

6. ISO/IEC 15026-1-2013, Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary

7. Transport for London (TfL), 2013. TfL Integrated Assurance Framework, Version 2. London

8. TfNSW Assets Standards Authority, 2016. Guide to Transport for NSW Framework for Assuring the Safety of Rail Assets and Infrastructure

9. TfNSW Assets Standards Authority, 2013. AEO Guide to Engineering Management, TS-10504

10. TfNSW Assets Standards Authority, 2013. Assurance and Governance Plan – Guidelines, T MU AM 00002 GU

11. NATO. 2010. Engineering for system assurance in NATO programs. Washington, DC: NATO Standardization Agency, DoD 5220.22M-NISPOM-NATO-AEP-67.

12. Aguilar, J. A, 2009. Design Assurance Guide, AEROSPACE REPORT NO. TOR-2009(8591)-11

13. INCOSE (International Council of Systems Engineering), 2015. Systems Engineering Handbook – A guide for System Lifecycle Processes and activities, 4th Edition, INCOSE-TP-2003-002-04

14. Hull, M. E. C., Jackson K., and Dick, J.J, 2005, Requirements Engineering, 2nd ed. Springer

15. Goal Structuring Notation Working Group, 2011 GSN Community Standard Version 1.1

Acmena

CONTACT US

+61 (0) 478 814 324
enquiries@acmena.com.au
www.acmena.com.au

Acmena Group Pty Ltd
PO BOX 220
Ashgrove West
Brisbane, QLD 4060
ABN: 37 158 514955
ACN: 158 514 955