Important message

This document is one of a set of standards developed solely and specifically for use on Transport Assets (as defined in the Asset Standards Authority Charter). It is not suitable for any other purpose.

The copyright and any other intellectual property in this document will at all times remain the property of the State of New South Wales (Transport for NSW).

You must not use or adapt this document or rely upon it in any way unless you are providing products or services to a NSW Government agency and that agency has expressly authorised you in writing to do so. If this document forms part of a contract with, or is a condition of approval by a NSW Government agency, use of the document is subject to the terms of the contract or approval. To be clear, the content of this document is not licensed under any Creative Commons Licence.

This document may contain third party material. The inclusion of third party material is for illustrative purposes only and does not represent an endorsement by NSW Government of any third party product or service.

If you use this document or rely upon it without authorisation under these terms, the State of New South Wales (including Transport for NSW) and its personnel does not accept any liability to you or any other person for any loss, damage, costs and expenses that you or anyone else may suffer or incur from your use and reliance on the content contained in this document. Users should exercise their own skill and care in the use of the document.

This document may not be current and is uncontrolled when printed or downloaded. Standards may be accessed from the Transport for NSW website at www.transport.nsw.gov.au

For queries regarding this document, please email the ASA at standards@transport.nsw.gov.au or visit www.transport.nsw.gov.au

© State of NSW through Transport for NSW 2019
Standard governance

Owner: Manager, Systems Engineering Process, Asset Standards Authority
Authoriser: Director, Network and Asset Strategy, Asset Standards Authority
Approver: Executive Director, Asset Standards Authority on behalf of the ASA Configuration Control Board

Document history

<table>
<thead>
<tr>
<th>Version</th>
<th>Summary of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>First issue</td>
</tr>
</tbody>
</table>
Preface

The Asset Standards Authority (ASA) is a key strategic branch of Transport for NSW (TfNSW). As the network design and standards authority for NSW Transport Assets, as specified in the ASA Charter, the ASA identifies, selects, develops, publishes, maintains and controls a suite of requirements documents on behalf of TfNSW, the asset owner.

The ASA deploys TfNSW requirements for asset and safety assurance by creating and managing TfNSW's governance models, documents and processes. To achieve this, the ASA focuses on four primary tasks:

- publishing and managing TfNSW's process and requirements documents including TfNSW plans, standards, manuals and guides
- deploying TfNSW's Authorised Engineering Organisation (AEO) framework
- continuously improving TfNSW's Asset Management Framework
- collaborating with the Transport cluster and industry through open engagement

The AEO framework authorises engineering organisations to supply and provide asset related products and services to TfNSW. It works to assure the safety, quality and fitness for purpose of those products and services over the asset's whole-of-life. AEOs are expected to demonstrate how they have applied the requirements of ASA documents, including TfNSW plans, standards and guides, when delivering assets and related services for TfNSW.

Compliance with ASA requirements by itself is not sufficient to ensure satisfactory outcomes for NSW Transport Assets. The ASA expects that professional judgement be used by competent personnel when using ASA requirements to produce those outcomes.

About this document

This document has been developed by the ASA and reviewed by members from TfNSW stakeholder groups.

This document aims to provide customer and supplier organisations with guidance through the steps involved in undertaking verification and validation activities that are used together for assuring that a product, service, or system fulfils its intended purpose.

This document forms part of a suite of systems engineering standards and guides and further develops the guidance on verification and validation described in T MU AM 06006 GU Systems Engineering Guide.

This document was previously issued as TS 10506 AEO Guide to Verification and Validation, version 1.0 in August 2013.
This document supersedes TS 10506 and is now issued as T MU AM 06016 GU Guide to Verification and Validation, version 1.0.

The changes from the previous issue include the following:

- change to document number and title
- minor amendments, updates and clarification to content
Table of contents

1. Introduction .............................................................................................................................................. 7
2. Purpose .................................................................................................................................................... 7
   2.1. Scope ..................................................................................................................................................... 7
   2.2. Application ............................................................................................................................................. 8
3. Reference documents ............................................................................................................................. 8
4. Terms and definitions ............................................................................................................................. 8
5. Verification and validation overview ..................................................................................................... 9
6. Verification ............................................................................................................................................. 10
   6.1. Verification activities ............................................................................................................................ 10
   6.2. Verification outputs .............................................................................................................................. 12
   6.3. Verification for software ....................................................................................................................... 13
7. Requirements verification and traceability matrix ............................................................................. 13
8. Validation ................................................................................................................................................ 14
   8.1. Validation activities .............................................................................................................................. 14
   8.2. Validation outputs ............................................................................................................................... 16
   8.3. Validation for software ......................................................................................................................... 16
1. **Introduction**

TfNSW, and any organisation undertaking engineering activities for TfNSW, is required to have verification and validation arrangements in place that are relevant to the engineering services or products that the organisation provides for TfNSW.

An engineering management plan, systems engineering management plan or equivalent plans and procedures describe how engineering activities are planned and managed so that the system will achieve agreed stakeholder requirements.

While this document applies to TfNSW and its supply chain, any organisation applying to be an AEO should ensure that its verification and validation activity and associated documentation meets the minimum level required for the complexity of its projects or contracts.

2. **Purpose**

This document describes the verification and validation processes, including key activities and responsibilities, expected to be implemented in managing verification and validation.

2.1. **Scope**

Mandatory verification and validation requirements are briefly defined for AEOs in T MU MD 00009 ST AEO Authorisation Requirements as follows:

*ENM11: "An AEO shall have arrangements for verification and validation management of the engineering services or products provided".*

This guide has been developed based on the technical processes of ISO/IEC/IEEE 15288:2015 *Systems and software engineering – System life cycle processes*, which are broadly intended to be used in the following manner:

- define the requirements for a system
- transform the requirements into an effective product
- use the product to provide the required services
- sustain the provision of those services
- dispose of the product when it is retired from service

This document provides an outline of the verification and validation processes that TfNSW and its AEOs need to demonstrate.
2.2. **Application**

This document is primarily intended for use by TfNSW and its supply chain, which includes all AEOs conducting engineering services undertaken for, or on behalf of, TfNSW.

3. **Reference documents**

The following documents are cited in the text. For dated references, only the cited edition applies. For undated references, the latest edition of the referenced document applies.

**International standards**


**Transport for NSW standards**

T MU AM 06004 ST Requirements Schema

T MU AM 06007 GU Guide to Requirements Definition and Analysis

T MU MD 00009 ST AEO Authorisation Requirements

**Other reference documents**

BKCASE 2018, Guide to the Systems Engineering Body of Knowledge (SEBoK)

4. **Terms and definitions**

The following terms and definitions apply in this document:

**AEO** Authorised Engineering Organisation

**ASA** Asset Standards Authority

**authorisation** the conferring of authority, by means of an official instruction and supported by assessment and audit

**RVTM** requirements verification and traceability matrix; alternatively referred to as requirements allocation and traceability matrix.

**TfNSW** Transport for NSW

**validation** confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

**verification** confirmation, through the provision of objective evidence, that specified requirements have been fulfilled
5. Verification and validation overview

Verification and validation are similar but distinct processes that are used together for assuring that a product, service, or system fulfils its intended purpose. The two processes are important for any project and are seen as essential in the life cycle of any complex system. The development of any system is not complete without ensuring that the implementation is consistent with the specifications.

Implementing verification and validation provides assurance that the product or service meets its required specifications, including any safety requirements. The outputs generated by the processes will form part of the assurance evidence supplied within product and system safety cases that lead to system acceptance and any necessary certification.

TfNSW and its AEO supply chain should ensure that its verification and validation arrangements meet the minimum level required for the complexity of its projects or contracts.

Verification and validation is undertaken through the full life cycle to ensure that the product or service correctly performs all its intended functions and that it does not perform any adverse unintended function.

All verification and validation activities, results and evidence should be recorded and traced in a structured repository or schema, as defined in T MU AM 06004 ST Requirements Schema.

System verification determines whether the system, its elements, and its interfaces satisfy their respective requirements and is undertaken throughout the plan and acquire stages, up to and including the integration phase.

Validation ensures that the final system meets all the stakeholder requirements and is typically undertaken through testing and commissioning during the later acquire stage, specifically during the acceptance phase, to enable system handover.

Figure 1 provides a high-level representation of the verification and validation activities during the plan and acquire life cycle stages up to system acceptance into operation.
6. Verification

System verification determines whether the system, its elements, and its interfaces satisfy their respective requirements. Therefore, verification applies to the system and subsystem requirements.

Verification checks the progress, conformance and effectiveness of an evolving solution by measuring compliance against requirements at each stage of development. Verification provides assurance that 'you designed it right, and you built it right'.

Verification demonstrates compliance to design requirements.

6.1. Verification activities

Verification activities associated with a system should typically include the following:

- defining a verification strategy
- defining a verification plan
- performing pre-verification checks
- performing verification

The output of the verification activities should be documented and recorded. These documents and records form part of the evidence supporting systems and safety assurance.
6.1.1. Defining a verification strategy

The verification strategy describes the verification processes that are required to demonstrate compliance with requirements.

The strategy incorporates continuous feedback of verification data that helps reduce risk and forces problems to surface early. The goal is to completely verify system capability to meet all requirements prior to integration and acceptance. The design of the verification activity should involve choosing the most cost-effective mix of activities to avoid unnecessary repetition of verification activities.

6.1.2. Defining a verification plan

A verification plan is based on the system requirements and outlines the activities that need to be performed for system verification. The verification criteria of the system requirements should be defined during the requirements analysis process. The basic forms of verification activities include the following:

- inspections
- analyses
- demonstrations
- tests
- certification

Inspection involves an examination of the item against documentation to confirm compliance with requirements. Inspection is used to verify properties best determined by examination and observation.

Analysis is the application of data, or performing simulations under defined conditions to provide data to show theoretical compliance. It is used where testing to realistic conditions cannot be achieved, or is not cost-effective. Analysis may be used when it can establish that the appropriate requirement, specification, or derived requirement is met by the proposed solution.

Demonstration involves a qualitative exhibition of functional performance. It is usually accomplished with minimal or no instrumentation. Demonstration is a set of test activities designed to show that the system or subsystem response to stimuli is suitable. Demonstration may be appropriate when requirements or specifications are given in statistical terms.

Tests are actions that verify the operability, supportability, or performance capability of an item under controlled conditions. Controlled conditions may be real or simulated. Tests often use special equipment or instrumentation to obtain quantitative data for analysis. The four basic test categories are:
- development test
- qualification test
- acceptance test
- operational test

Certification comprises a special form of verification against established legal or industrial standards. Certification is performed by an external authority without direction to that authority as to how the requirements are to be verified. For example; certification is used for electronic devices for CE (Comité Européen) certification in Europe, UL (Underwriters Laboratory) certification in the US and Canada, and C-tick certification in Australia.

6.1.3. Performing pre-verification checks

Pre-verification checks are performed to ensure the system for verification is available and that any associated facilities, equipment and operators are prepared to conduct the verification.

In some situations, independent verification may be required. This may be performed by another part of the design organisation that is not involved in the design, or by a separate organisation.

Where independent verification or stakeholder witnessing is required, these parties will require advanced copies of the verification plans, documents and verification program.

6.1.4. Performing verification

Conduct verification activities to demonstrate compliance to the relevant design requirements.

Results from verification activities should be analysed, recorded, and reported to stakeholders. Any requirements verification and traceability documentation should be updated with the verification status and results. Where verification has been unsuccessful, corrective action procedures should be developed and implemented.

Refer to Section 7 for information about the requirements verification and traceability matrix.

6.2. Verification outputs

The output of the verification process is the demonstration through the recording of evidence that the product satisfies the system and subsystem requirements, stakeholder requirements have been met, and any corrective actions have been identified and resolved.

Where full verification against a requirement cannot be achieved, the appropriate noncompliance or concession should be applied for following the agreed project procedures.
Noncompliances and concessions should be applied for at the earliest opportunity. This could be during the plan and acquire stages of a project life cycle and should be approved prior to the next life cycle stage gateway.

Refer to Section 7 for information about the requirements verification and traceability matrix (RVTM).

6.3. Verification for software

Rigorous verification processes are required where software is involved, particularly in the case of mission or safety-critical control, communication and signalling elements. Software verification processes include additional verification methods other than testing alone, since testing in general cannot completely show the absence of errors. The software verification process is usually a combination of review, establishment of traceability, analyses, and testing.

Reviews and analyses are performed on the following components:

- software requirements - to detect and report requirements errors that may have been uncovered during the design process
- software architecture - to detect and report errors that occurred during the development of the software architecture
- source code - to detect and report errors that may have developed during source coding
- outputs of the integration process - to ensure that the result of the software integration process is complete and correct
- test cases and their procedures and results - to ensure that the software testing is performed accurately and comprehensively

Regression testing is essential when a software change is made to ensure that no adverse effects to other dependent elements of the system are introduced.

Configuration management of software verification is also essential, particularly during software integration testing, to ensure that configuration of the elements and systems combined together is both representative and of value to the final system.

7. Requirements verification and traceability matrix

The requirements definition and analysis process should have established a requirements verification and traceability matrix (RVTM). This RVTM should list all of the stakeholder requirements, their verification attributes, and traceability back to the source.

The RVTM may be implemented in a spreadsheet for simpler projects, but is often part of a requirements schema implemented using specialised requirements management software tools.
TfNSW currently uses IBM DOORS to manage its requirements and associated verification and validation records on complex transport projects, but this tool is not mandated on the supply chain.

The RVTM should include fields for the verification status, a reference to the location of verification evidence, and the level of the system's compliance to each requirement.

The RVTM should be progressively updated after completion of verification activities.

A list of attributes that typically feature in a RVTM is included in T MU AM 06007 GU Guide to Requirements Definition and Analysis.

Generic verification process flow charts are contained in the Guide to the Systems Engineering Body of Knowledge (SEBoK).

As projects increasingly use digital engineering, requirements management and verification and validation management will become increasingly integrated with digital engineering.

8. Validation

Validation ensures that the final system meets all of the stakeholder and user requirements that were captured at the outset, and any approved changes or additions to those requirements. Therefore, validation applies to meeting the business requirements.

Validation confirms that a system performs as it was intended to perform and that the system does not perform in an unacceptable manner, or produce unacceptable results or outcomes. Validation provides assurance that 'you built the right thing'.

Validation activities generally involve the active participation of end-users and all relevant stakeholders as a part of the element and system testing processes. Design and construction deliverables will typically be validated in addition to end-state systems and products, including all element and system interfaces. This validation process requires the use of simulation, review and site checks to obtain stakeholder acceptance at the appropriate stage of the 'V' life cycle.

Validation may be performed in the actual operational environment or a simulated operational environment if real-world conditions are too hazardous for validation observers.

8.1. Validation activities

End-users and other stakeholders usually participate in validation activities.

Validation activities should typically include the following:

- defining a validation strategy
- defining a validation plan
• performing pre-validation checks
• performing validation

The output of the validation activities should be documented and recorded as evidence. These documents and records form part of the evidence supporting systems and safety assurance.

8.1.1. **Defining a validation strategy**

A validation strategy may involve using independent third parties to perform validation. These third parties may come from another part of the design organisation not involved in the design, or a separate organisation.

Where independent validation or stakeholder witnessing is required, advanced copies of the validation plans, documents and validation program are to be made available to those parties.

8.1.2. **Defining a validation plan**

A validation plan is based on the user and stakeholder requirements. The validation criteria of user and stakeholder requirements should be defined during the requirements analysis process.

Testing is the preferred method of system validation, either as standalone tests, or in combination with analysis techniques in cases where it is not possible or feasible to test over the entire operating spectrum.

Typical validation activities may include the following:

• demonstration
• inspection
• tests
• analysis

Demonstration involves a qualitative exhibition of functional performance, usually accomplished with no or minimal instrumentation.

Inspection comprises an examination of the item against documentation to confirm compliance with stakeholder or user requirements.

Tests are actions by which the operability, supportability, or performance capability of an item is verified when subjected to controlled conditions that are real or simulated.

Analysis includes techniques such as mathematical modelling, finite-element analysis and computer-based simulation, in addition to the use of physical simulators. Analysis is a method of system validation applied only in circumstances where no other form of validation activity is logistically manageable or safe to undertake.
8.1.3. Performing pre-validation checks

Pre-validation checks are performed to ensure the system to be validated is available and that any associated facilities, equipment and operators are prepared and able to conduct the validation.

8.1.4. Performing validation

Validation activities are conducted to demonstrate compliance to stakeholder requirements and are performed in the operational environment or a simulated operational environment when real-world conditions are too hazardous for validation observers.

Where validation has been unsuccessful, corrective action procedures should be developed and implemented.

Refer to Section 7 for information about the requirements verification and traceability matrix.

8.2. Validation outputs

When the validation activities are completed, then the validation results are recorded, analysed and reported. The requirements verification and traceability matrix should be updated with the validation status and results.

The output of the validation process is intended to demonstrate that the final system satisfies all of the stakeholder and user requirements. Validation outputs can be demonstrated through recording demonstration, inspection, tests and analysis evidence such that the services provided by the system required by the stakeholder have been achieved and that any corrective action has been identified and resolved.

Where full validation against a requirement cannot be achieved, the appropriate noncompliance or concession should be applied for using the agreed project procedures. Noncompliances or concessions should be requested at the earliest opportunity. This could be during the plan and acquire stages of a project life cycle and should be approved prior to the next life cycle stage gateway.

8.3. Validation for software

Where software is involved, as is the case with safety-critical control, communication and signalling elements, rigorous validation processes are required. The main objective of software validation is to demonstrate that the elements and system satisfy all of the requirements, and that errors leading to unacceptable failure conditions are removed.

Software validation processes typically include the following:

- software module testing - to confirm that software modules function correctly
- element level testing - to confirm that elements function correctly when modules are combined together into elements
- hardware and software integration testing - to confirm that the software is operating correctly in the computer environment
- system element modelling and simulation - to validate through the use of element and system level models and simulations that the proposed design will achieve all the stakeholder requirements including operations and maintenance
- software integration testing - to confirm the interrelationships between the software requirements and components, and to validate the implementation of the requirements and components in the software architecture