Complex system integration in railways

RISSB
RAIL INDUSTRY SAFETY AND STANDARDS BOARD

Safety Standard

Please note this is a RISSB Australian Standard® draft

Document content exists for RISSB product development purposes only and should not be relied upon or considered as final published content.

Any questions in relation to this document or RISSB's accredited development process should be referred to RISSB.

RISSB Office

Phone:	**Email:**	**Web:**
(07) 3724 0000 Overseas: +61 7 63724 0000	info@rissb.com.au	www.rissb.com.au

Standard Development Manager Contact

Name: Jesse Baker Phone: 0419 140 580 Email: jbaker@rissb.com.au

This Australian Standard® AS 7473 Complex system integration in railways was prepared by a Rail Industry Safety and Standards Board (RISSB) Development Group consisting of representatives from the following organisations:

Acmena	Amoq Consulting	Asset Standards Authority Australia
Aurecon	BHP Billiton	CWQ Consulting
Metro Trains	Public Transport Victoria	Public Transport Authority of Western Australia
Rail Assurance Consulting	Siemens	Transport for New South Wales
University of Central Queensland	University of Wollongong	WSP

The Standard was approved by the Development Group and the Enter Standing Committee Standing Committee in Select SC approval date. On Select Board approval date the RISSB Board approved the Standard for release.

Choose the type of review

Development of the Standard was undertaken in accordance with RISSB's accredited process. As part of the approval process, the Standing Committee verified that proper process was followed in developing the Standard

RISSB wishes to acknowledge the positive contribution of subject matter experts in the development of this Standard. Their efforts ranged from membership of the Development Group through to individuals providing comment on a draft of the Standard during the open review.

I commend this Standard to the Australasian rail industry as it represents industry good practice and has been developed through a rigorous process.

Chief Executive Officer
Rail Industry Safety and Standards Board

Keeping Standards up-to-date

Australian Standards developed by RISSB are living documents that reflect progress in science, technology and systems. To maintain their currency, Australian Standards developed by RISSB are periodically reviewed, and new editions published when required. Between editions, amendments may be issued. Australian Standards developed by RISSB could also be withdrawn.

It is important that readers assure themselves they are using a current Australian Standard developed by RISSB, which should include any amendments that have been issued since the Standard was published. Information about Australian Standards developed by RISSB, including amendments, can be found by visiting www.rissb.com.au.

RISSB welcomes suggestions for improvements and asks readers to notify us immediately of any apparent inaccuracies or ambiguities. Members are encouraged to use the change request feature of the RISSB website at: http://www.rissb.com.au/products/. Otherwise, please contact us via email at info@rissb.com.au or write to Rail Industry Safety and Standards Board, PO Box 518 Spring Hill Qld 4004, Australia.

Notice to users

This RISSB product has been developed using input from rail experts from across the rail industry and represents good practice for the industry. The reliance upon or manner of use of this RISSB product is the sole responsibility of the user who is to assess whether it meets their organisation's operational environment and risk profile.

AS 7473:2019

Complex system integration in railways

Document details

First published as: Enter first publication identifier (AS XXXX:yyyy)

ISBN Enter ISBN.

Document history

Publication Version	Effective Date	Reason for and Extent of Change(s)
2019	Select Board approval date	

Draft history (Draft history applies only during development)

Draft version	Draft date	Notes
Draft for Public Comment	05/08/2019	

Approval

Name	Date
Rail Industry Safety and Standards Board	Select Board approval date

Copyright

Published by SAI Global Limited under licence from the Rail Industry Safety and Standards Board, PO Box 518 Spring Hill Qld 4004, Australia

This Standard was prepared by the Rail Industry Safety and Standards Board (RISSB) Development Group AS 7473 Complex system integration in railways. Membership of this Development Group consisted of representatives from the organisations listed on the inside cover of this document

Objective

The objective of this Standard is to establish the processes necessary to enable the management of risk in the integration of complex systems in the railway environment.

This Standard is applicable to both the acquirer and supplier organisations and can be used where either a single entity or multiple parties are engaged.

The principles of systems integration outlined in this document can be used to establish the business environment, e.g. methods, procedures, tools, and organisational structure for parties engaged in delivering complex projects in the railway environment….

Compliance

There are two types of control contained within Australian Standards developed by RISSB:

1. Requirements.
2. Recommendations.

Requirements – it is mandatory to follow all requirements to claim full compliance with the Standard. Requirements are identified within the text by the term 'shall'.

Recommendations – do not mention or exclude other possibilities but do offer the one that is preferred. Recommendations are identified within the text by the term 'should'.

Recommendations recognise that there could be limitations to the universal application of the control, i.e. the identified control is not able to be applied or other controls are more appropriate or better.

For compliance purposes, where a recommended control is not applied as written in the standard it could be incumbent on the adopter of the standard to demonstrate their actual method of controlling the risk as part of their WHS or Rail Safety National Law obligations. Similarly, it could also be incumbent on an adopter of the standard to demonstrate their method of controlling the risk to contracting entities, or interfacing organisations where the risk may be shared.

Controls in RISSB standards address known railway hazards are addressed in an appendix.

Contents

Appendix Contents

1 Scope and general

1.1 Scope

This Standard provides a framework of processes for the identification and mitigation of risks arising from the introduction of systems in the railway environment. It establishes the principles and methodologies that can be applied at any level of the hierarchy of a system structure throughout the system lifecycle. This is achieved through the engagement of stakeholders to establish their role and the allocation responsibilities to these parties to support delivery of the objective(s) set out by the organisation or project.

This Standard provides processes to support the definition, control and optimisation of integration processes used within an organisation or project that can be applied by the adopter when procuring or delivering systems.

This Standard defines the management processes, based on a system lifecycle, for risks associated with the design and implementation of both hard and soft systems in the railway environment whose interfaces may be: commercial, data, logical, human, or physical in nature.

Operational integration risks can occur from introduction of hard or soft systems to the railway environment. Where this occurs, the management of the operational integration risks shall, in conjunction with this Standard, be reviewed by the responsible organisation or project through the development of concept of operation, and concept of maintenance documentation supported by an operational integration strategy specific to the context of application.

1.2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document:

- AS/NZS ISO/IEC/IEEE 15288, Systems and software engineering — System life cycle processes
- AS/NZS ISO/IEC 12207, Systems and software engineering -- Software life cycle processes
- AS/NZS ISO 9001, Quality management systems – Requirements
- IEC 62278 (all parts), Railway Applications Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
- EN 50126-1, Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). Generic RAMS Process

NOTE: Documents for informative purposes are listed in a Bibliography at the back of the Standard.

1.3 Terms and definitions

For the purposes of this document, the following terms and definitions apply:

(a) ***acquirer***
Stakeholder that acquires or procures a product or service from a supplier.

(b) ***adopter***
Stakeholder that assumes in part or in full the requirements and recommendations set by this standard.

(c) ***complex system***
A system composed of multiple system elements which interrelate and are interdependent (Integrate) from one another. The integration of the system elements forms the system. Complex Systems often exhibit numerous emergent properties.

(d) ***interface***
A point of interaction between parties or subsystems during a system or subsystem life-cycle phase.

(e) ***rail infrastructure manger (RIM)***
In relation to rail infrastructure of a railway, means the person who has effective control and management of the rail infrastructure, whether the person owns the rail infrastructure; or has a statutory or contractual right to use the rail infrastructure or to control, or provide, access to it.

(f) ***rail safety regulator***
The National Rail Safety Regulator or an acting national rail safety.

(g) ***responsible organisation***
The organisation authorised and/or accountable.

(h) ***SMART criteria***
A criteria for system integration requirements. The requirement should be specific, measurable, attainable, relevant, and time bound.

(i) ***system***
Specifically defined combination of interacting elements, organized to achieve one or more stated purposes. Each system can be composed of lower-level systems (subsystems).

(j) ***systems engineering***
Interdisciplinary approach governing the total technical and managerial effort required to transform a set of stakeholders' needs, expectations, and constraints into a solution and to support that solution throughout its life.

(k) ***systems integrator***
The party responsible for integrating the subsystems/elements that make up the system.

(l) ***safety***
Freedom from unacceptable risk of harm.

(m) ***TRAK***
An open source systems engineering enterprise architecture framework.

General rail industry terms and definitions are maintained in the RISSB Glossary: https://www.rissb.com.au/products/glossary/

2 Key concepts for this Standard

2.1 System boundaries

The language and nature of a project changes depending on the definition of the system concerned. The primary activity, and risk mitigation exercise, of any project is to determine the system and its boundaries. Definition of the system boundaries enables for a common understanding between the acquirer and the supplier, on the system-of-interest. Once these are agreed, activities involving other parties are immediately less ambiguous, noting that boundary changes can occur over time, but the definition of an initial understanding of the boundary often precipitates the discussion necessary to refine it, and enables any subsequent change control required.

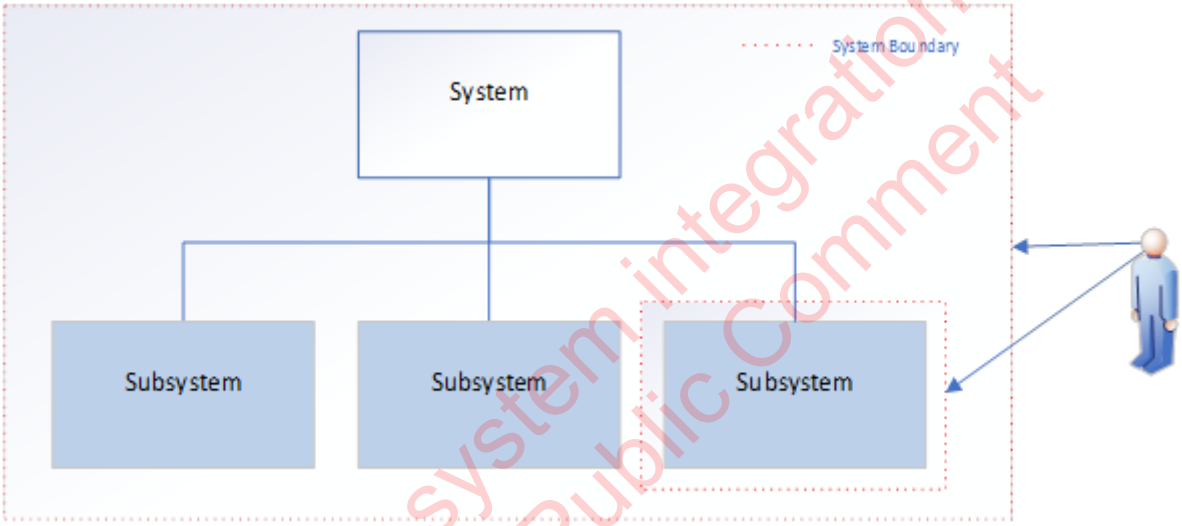

Figure 2.1: Illustration of System Boundaries

Note that the precise boundaries can be unobvious – e.g. signalling assets are often found inside rolling stock, and even then, some assets (display equipment) may be shared. For this reason, the functional boundary can provide a better definition than the physical boundary; and, either way, a case like this makes evident the reason for defining those boundaries early.

The interpretation of this Standard can change depending on system and its boundary. It is broadly assumed that this Standard will be applied to large projects, where the system is composed of multiple, individually-complex subsystems, being integrated to deliver the business capabilities to be realised.

In any case, the boundary definition shall carefully regulate the depth of detail. Ensuring that this tiered approach to system build-up is adhered to avoids the importing of unnecessary and distracting levels of detail into any evaluation. It also ensures that focus on resolving issues remains where the expertise is generally found (i.e. the rolling stock supplier remains responsible for issues entirely within the supply of the rolling stock).

Defining and agreeing those boundaries aligns to this approach, as well as the standardised approaches to safety management, reliability, operability and so on.[1]

[1] iESM, EN 50126-1:2017 and EN50126-2:2017.

Every project team shall identify the scope of the system for which they are responsible, the subsystems it is composed of, and their scopes respectively.

If a project team is responsible for multiple systems, each system and/or subsystem shall be identified and treated individually.

Project teams may exist in the originating agency, delivery agencies and throughout the supply chain.

In the context of this section, each project team shall be responsible for the scope for which they are assigned, or ensure that a capable party is given the responsibility in their stead. This includes the determination of how that scope is broken down, integrated and delivered.

2.2 Integration in the system life cycle

This Standard defines the progressive management processes that enable the control of system integration factors specific to railway applications in alignment to the system lifecycle, see Appendix B.

Systems are typically described as a hierarchy of interdependent elements which, through their interaction, deliver an intended capability. This “divide and conquer” approach to developing systems that is well documented by other International Standards, provides an optimised approach in the utilisation of resources, and fosters innovation when developing systems. Integration concerns the method by which system elements delivered through this approach are brought together to ensure they deliver the anticipated system emergence within the environment for which the overall system has been designed. Therefore, system integration shall be undertaken progressively concurrently with other systems engineering activities across all system lifecycle phases.

Integration activities shall begin at the conception of the system and be imbued across the system lifecycle as shown in Figure 2.2. The definition and planning phases of the system shall be used to develop a procurement strategy that reduces complexity and minimises potential commercial dependencies between system elements. An integration management strategy shall be developed by the acquirer to outline an approach for managing integration risks emanating from their system delivery model and the context in which the system is to be integrated. The acquirer shall define the processes by which the resulting system is incorporated in its operational environment. The acquirers’ integration strategy shall define the processes by which coordination and collaboration between supplier organisations shall be managed throughout the system lifecycle.

Supplier organisations shall develop and be responsible for the identification and management of integration risks for elements of the system within their control.

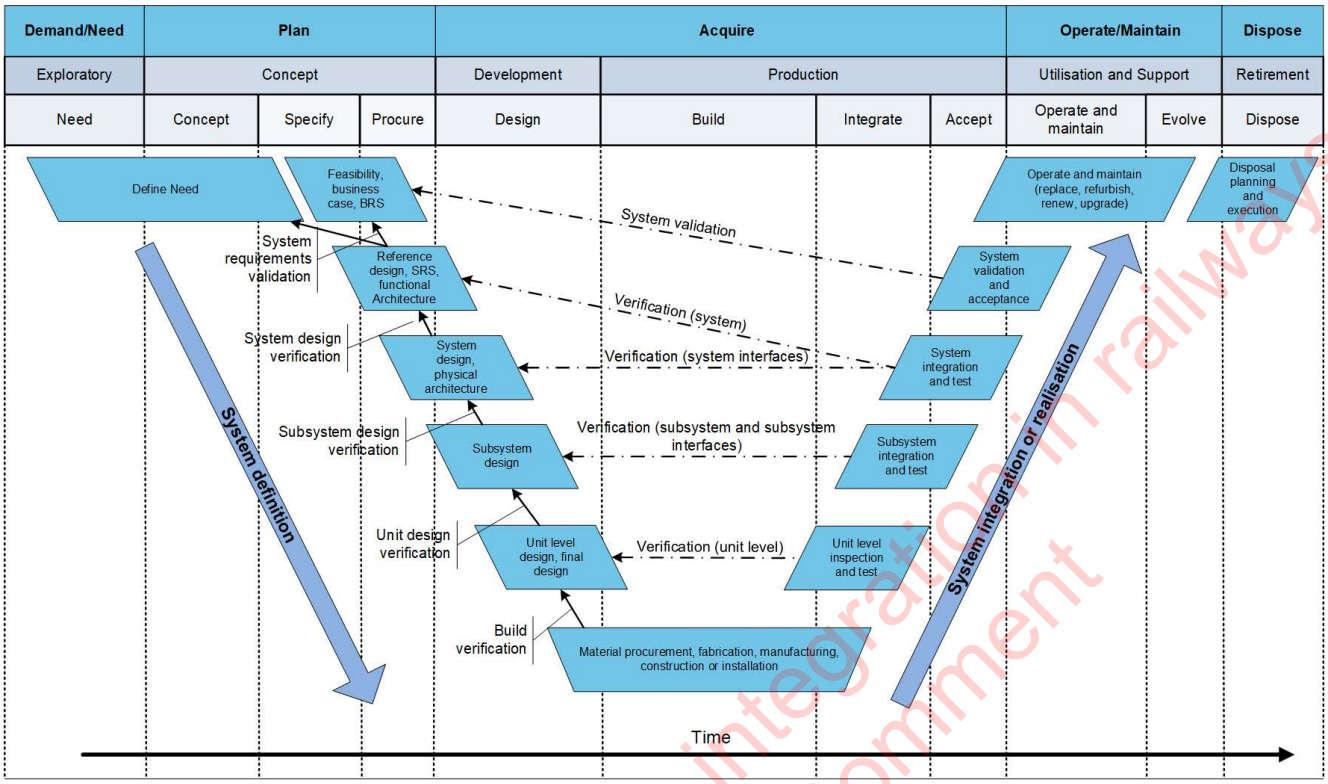

Figure 2.2 System Integration activities in a typical system lifecycle

2.3 System integration organisation

2.3.1 General

It is not sufficient to integrate sideways (splitting a scope up and asking each party to collaborate), at least one party shall look vertically (top down); ideally the acquirer or an allocated systems Integrator. The acquirer / system integrator shall ensure that emergent properties and top-level objectives are reached, and that brokering between parties leads to useful and unbiased results. Note: it is here that the expertise of the acquirer / system integrator is evident (e.g. the operator) or, at least, a strong liaison is established.

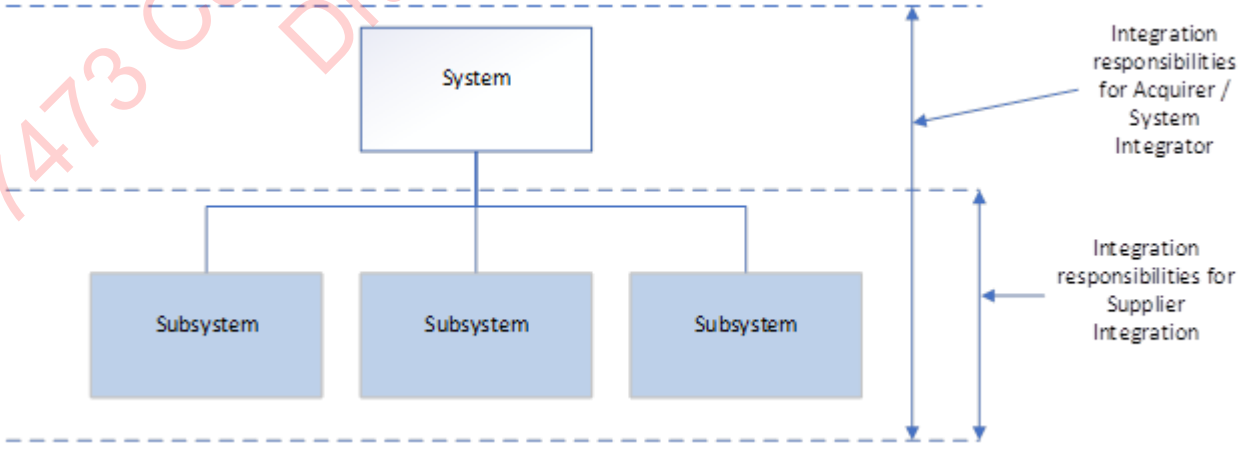

Figure 2.3 Typical distribution of integration responsibilities

It can be assumed that the bottom-up aspect will be provided by the suppliers themselves, and this view is well-covered.

The acquirer shall, within their integration strategy set out a framework for the governance of integration activities throughout the system lifecycle. The governance framework shall describe the extent of authority and responsibility for integration activities allocated to both the supplier and acquirer organisations.

2.3.2 Functions of systems integration organisation

The system integration organisation should be drawn from both the acquirer and supplier organisations. This is intended to foster a collaborative interdisciplinary entity that is cognizant of the scale and scope of the undertaking. Typical functions within the integration organisation will include but not be limited to:

(a) acquirer / system integrator representative;

(b) interface manager;

(c) design managers from both the supplier and acquirer organisation;

(d) user and maintenance representatives.

The structure of the system integration organisation is reflective of the environment in which it is operating. Therefore, it is important that the organisation has sufficient understanding of the system itself, the context in which the system is being delivered and is adequately resourced (and capable) to conduct and manage the anticipated integration activities.

2.4 Competency management

Each organisation participating in integration activities throughout the system lifecycle shall ensure persons conducting integration roles have the professional judgement and are competent to produce the intended outcomes. The organisation shall ensure persons responsible for the management of interfaces demonstrates the competencies to deliver their role.

Responsibility for assessing competent lies within the requirements of the organisations jurisdiction. The Rail Transport Operator (RTO) should consider an appropriate distribution of workload necessary to deliver project objectives with regards the management of integration activities.

2.5 Stakeholder engagement

Stakeholder engagement within the integration lifecycle is undertaken not only to establish and develop communications with parties affected by the anticipated emergence of the system in development but to obtain information necessary for the analysis and categorisation of interfaces in latter stages of design.

Stakeholder management practices and their use are sufficiently described elsewhere and are not be discussed here. However, where applied, organisations responsible for system integration shall use these processes to identify and communicate the effect of changes to interfaces at their system boundary to affected stakeholders. This is especially important where such changes have implications on the stakeholder's organisation or introduce constraints to other system elements.

2.6 Information management

The integration strategy shall define the systems and methods that will be employed for managing information arising out of integration activities (including the production and preservation of records), managing information flows (assurance chain) and for managing configurable items. The integration strategy shall, as a minimum:

define an agreed information interchange format before the project commences;

establish how information will be used by the end-users to ensure the systems can be managed and maintained for the duration of the system lifecycle.

Information management processes shall define the processes by which residual risk emanating from the control of integration risks are communicated, transferred, and accepted by the operating organisation.

2.7 System migration

Migration planning is a complementary system engineering technique used to identify the staging activities undertaken in deploying a system. It is used to define the interim states in which system interfaces can/will change throughout the system lifecycle. Such an approach is considered useful where integration concerns changes to in-service systems or the introduction of new systems to brownfield environments. Here, migration strategies are used to identify the interdependency logic between system elements and establish the enabling functions required to support each transition.

Therefore, the responsible organisation shall develop a strategy for the management of enabling works, stage works, temporary and fringe works where system interfaces exist. The responsible organisation shall also develop recovery strategies where system interfaces can fail during integration activities.

During migration planning of systems development for the end-state, the responsible organisation shall support the acquirer organisation in their preparation (organisational readiness) for the integration of systems in the operational environment.

The delivery organisation should during the system integration phase cater for various User training and assess the utilisation of the system of interest. The acquirer organisation should plan the business migration accordingly from a legacy system into a new operational system.

3 System integration

3.1 Planning for integration

3.1.1 Strategy

A system integration strategy shall be developed by the responsible organisation in the definition and planning stages of the system lifecycle. The scale of the integration management strategy shall be dependent on the magnitude of the risk and complexity of the project. The integration strategy shall define the processes by which system interfaces are to be identified, analysed, controlled, and managed across the system lifecycle in accordance to ISO/IEC/IEEE 15288.

System integration planning shall as a minimum, address the following:

(a) Definition of the system boundary and the identification of interacting systems.

(b) The structure of the systems integration organisation.

(c) The governance of the integration organisation including their extent of authority and responsibilities.

(d) The system integration lifecycle setting out activities to be conducted by the system integration organisation.

(e) The associated deliverables generated by such activities.

(f) Method by which the integration processes are to be verified and validated throughout the system lifecycle.

3.1.2 Identifying system interfaces

Abstractions or architectures should be used to better identify the system-of-interests' relationship with its environment and other systems. Various techniques for achieving this, e.g. TRAK, are documented elsewhere though none are prescribed by this Standard. Interfaces are the functional, physical, or informational characteristics that exist at common boundaries between items. The identification of system interfaces requires some understanding of context in which the system-of-interest is intended to / currently operates.

3.1.3 Interface control

3.1.3.1 Definition of system interfaces

The systems integration organisation shall be responsible for gathering and defining the system-of-interests interfaces. These interface definitions shall be updated regularly and reviewed at each design stage gate. The system integration organisation shall create documentation as per Clause 5 of this Standard to describe the interfaces between each of the systems that make up the overall architecture of the system-of-interest. Such documentation shall continue to be developed as the design matures so the lower level interfaces can be identified and defined. External interfaces should be captured through regular stakeholder engagement activities where interfacing projects / undertakings exist.

System interfaces shall, as a minimum, be identified, defined, and categorised as follows:

(a) Functional: those in which events in one system trigger an outcome / event(s) in other.

(b) Physical: a mechanical or structural link between system elements.

(c) Information: those over which information is exchanged.

(d) Logical: groupings by convention.

3.1.3.2 Interface analysis

Interface analysis should consider the extent and nature of interactions across system interfaces. Such an analysis shall be used to determine the risks and associated controls to manage all risks emanating from system interfaces. Analysis of system interfaces shall also be used to determine ownership of system interfaces. This should be conducted collaboratively with the relevant stakeholders to provide assurance that the scope and extent of ownership for system interfaces is understood.

Risk analysis with respect to system interfaces shall evaluate the following:

(a) Any known areas of potential high risk or possible non-compliance.

(b) Inputs from other risk assessment activities.

(c) Surveillance activities pertaining to the project conducted on the supplier e.g. audits, inspections etc.

The outcome of interface analysis shall be documented in the appropriate risk register and the conclusions summarised in the relevant assurance records. Requirements derived from controls developed to manage safety-related risks pertaining to system interfaces shall be managed through the responsible organisations requirements management strategy. The responsible organisation shall also apply the information management framework documented by their integration to communicate the risks associated with the interfaces in their domain.

3.1.3.3 Assigning responsibility for interfaces

Interface definition documentation shall be created for each identified interface. The allocation of responsibility for the creation and maintenance of these documents shall depend on the level of integration required for the respective interface. It is expected that:

(a) where the interface is entirely within the scope of a single system, the responsible supplier shall allocate an engineer from within that system-of-interests scope to manage the interface;

(b) where the interface is between two systems, an Engineer shall be nominated by the responsible suppliers' design management forum to manage the interface across both systems-of-interest. The appointed engineer should be part of the leading system in the interface where such an arrangement exists;

(c) where the interface is between multiple systems an Engineer shall be nominated by the systems integrator / acquirer organisation who resides in that organisation.

The systems integration organisation shall be responsible for reviewing each of the interfaces and their associated documentation, including those describing the interfaces between suppliers.

3.2 Design management

3.2.1 Strategy

The responsible organisation shall develop an overarching design management strategy to define the process through which design activities will be managed across the system lifecycle for the system-of-interest. Where responsibilities are devolved to supplier organisations, it is expected that each party shall document a complementary strategy to define the methods by which design activities are to be delivered across the systems within their scope of works.

The design management strategy shall document the overall scope, project lifecycle and breakdown structure for the works to be delivered by the responsible organisation. The strategy should outline the delegation of design responsibilities between the various supply organisations and document how the respective undertakings will contribute to the delivery of the overall program.

The design management strategy shall also describe the design control process, design control points and the anticipated exit criteria for each control point.

3.2.2 Designing interfaces

Designing interfaces shall align with the system integration management plan. The following task shall be undertaken:

(a) Identify and comply with the relevant standards.

(b) Identify and define the correct operation of the assembled interface.

(c) Identify and plan for enabling systems that support system / subsystem synthesis. The enabling system shall meet the desired functions and shall be verifiable.

(d) Identify system interface constraints and plan where appropriate.

(e) Identify human-centred interfaces.

(f) Identify and review interoperability and scale between system elements.

3.2.3 Risks, assumptions, issues and dependencies

The responsible organisation shall develop processes to manage the risks, assumptions, issues, and dependencies associated with the development of the system-of-interest. Each entry documented though this process, be it a risk, assumption, issue, or dependency, should be assigned to an appropriate owner and provide the relevant actions required to implement an effective resolution and closure of the entry within a given timeframe.

3.2.4 Design reviews and approvals

The responsible organisation shall identify control points in the design phases at which a design freeze shall be taken and a system level review performed. The control points are those at which the supplier organisations shall come together to review and evaluate the progress of the overall systems' development with the system integrator / acquirer. The control points are expected to facilitate better management of the design, ensure timely delivery of design packages, and progressively assure work package integration and technical interface issues.

Design reviews and controls points shall align with the responsible organisations assurance strategies, Clause 4 and satisfy the requirements of the relevant jurisdiction in which the project is delivered.

3.3 Requirements management

Interface requirements shall be generated using outcomes of analysis activities described in Clause 3.1.2.2. To achieve this, the responsible organisation shall implement a robust requirements management process and provide the necessary resource to manage the requirements.

The requirements management process shall be catered for through the whole system lifecycle. The following objectives should be achieved during project initialisation:

(a) A common agreement (between the acquirer and supplier) on key requirements characteristics and attributes, to be managed during the project lifecycle.

(b) A common understanding on the system requirements, (functional, non-functional, interface, performance, safety, security, human factor, electromagnetic interference), this is different to the project requirements (management, statement of work etc).

(c) A common understanding on key definition to be used throughout the project lifecycle and the system lifecycle. (Glossary)

(d) A common acceptance criteria on requirement verification during the design phase.

The following objectives should be achieved during project design development:

(a) A throughout understanding of the system capabilities to be delivered, through the decomposition of technical requirements within each system-of-System and/or subsystems.

(b) A common acceptance criteria the validation of requirements be conducted during system testing and commissioning.

(c) A common agreement on derived safety related requirements.

The following objectives should be achieved prior to system integration:

(a) A map out and traceability satisfaction from the high-level requirement, down to the system and/or subsystem level.

(b) Interface requirements agreement between parties involved.

During the system integration evidence from testing and commissioning shall validate the requirement acceptance criteria.

3.4 Reliability, availability, maintainability

The responsible organisation shall develop a reliability, availability and maintainability (RAM) strategy to describe the method by which RAM tasks are to be applied to the system-of-interest in accordance to EN 50126-1.

The RAM strategy should set out the process to validate whether the architecture of the system-of-interest can deliver the reliability performance set by the acquirer's requirements.

3.5 Configuration management

To manage the risks of delivering multiple systems to differing timescales, rigorous control shall be maintained on the technical, program and commercial baselines. The responsible organisation shall identify control points and system review processes as outlined in Clause 3.2.3.

At each control point, the suppliers should prepare a baseline report of all critical design products for review by the system integrator / acquirer organisation. The baseline report should provide a reasoned and evidenced argument for the satisfactory system assurance for the respective suppliers' system-of-interest. As a minimum, the baseline report should document the status of the following artefacts:

(a) Requirements and verification evidence.

(b) Risk registers.

(c) System architectures and key interfaces.

(d) System migration roadmap and key dependencies.

(e) System Safety Hazard register and agreement on risk allocation.

(f) Register of applicable standards and any identified non-conformances.

The outcome of control point reviews should lead to the allocation of remedial actions to an owner and a timescale for their completion. Intermediate reviews may be held between control points where the progress of the remedial actions requires additional monitoring.

3.6 Safety in design

The responsible organisation shall, in accordance with Rail Safety National Law, establish an engineering safety management strategy that defines the safety processes to be followed in delivering the system-of-interest.

The engineering safety management approach shall document the activities through which hazards associated with system interfaces are to be identified, and the associated risks controlled, and managed. Such activities shall review hazards and associated risks emanating from interfaces across the whole of the system lifecycle.

3.7 Relationship with the supply chain

As stated in Clause 2.3, the integration of systems delivered by multiple organisations requires that at least one party be responsible for the overall integration of the system. Ideally, such responsibilities are accorded to the acquirer or an allocated Systems Integrator. The acquirer / System Integrator shall be responsible of ensuring the overall systems emergent properties and objectives are achieved by brokering between suppliers.

Where a system has been contracted to a supplier, the supplier shall be responsible for integrating the sub-elements of the system within their scope and providing the necessary assurance to the acquirer / System Integrator that their system-of-interest delivers the objectives set out by their scope. Each supplier shall provide documentation pertaining to their system-of-interest interfaces (Clause 5) necessary to facilitate integration of their system with other elements. The supplier shall also provide the necessary assurance evidence to demonstrate compliance with the requirements for performance (Clause 3.4) and safety (Clause 3.6) associated with all interfaces for their system-of-interest.

Each supplier should also avail the resources allocated to manage the interface(s) (Clause 3.1.2.3) to support integration activities conducted by adjacent systems.

3.8 Testing and commissioning

Testing and commissioning of the integrated system shall be conducted at the appropriate system lifecycle by the responsible supplier to demonstrate compliance to the relevant customer requirements. Each supplier shall apply the verification methods specified for each requirement within the scope of their system-of-interest as set out in Clause 4.2. Testing and commissioning shall be conducted in stages, as the systems are integrated progressively, in accordance with the system lifecycle and schedule.

Any defects or faults identified through the testing and commissioning activities shall recorded and managed through the failure reporting and corrective action system or equivalent processes set out in Clause 4.3.

3.9 Operational integration

Planning for operational Integration shall include the following:

(a) Define the operational integration requirements with the governing body and the operator.

(b) Identify the risks, controls, and risk owners.

(c) Develop an operational integration strategy and timeline.

(d) Define operational constraints.

(e) Identify the functions and responsibilities that are required and allocate to appropriate resources.

(f) Define appropriate deliverables and milestones.

(g) Develop an Operational Integration plan of approach for the activities related to Operational Integration. This should include a functional organisational chart, work-breakdown structure and cost-breakdown for each activity.

(h) Define operational integration critical success factors.

(i) Identify and consult with end-users to further develop the requirements.

4 Systems assurance

4.1 Assurance strategy

The assurance strategy should aim to progressively gather and provide assurance evidence to demonstrate whether, at key lifecycle gateways, the system being developed / commissioned / delivered achieves the following:

(a) Reliability, availability & maintainability targets.

(b) Identified safety risks are reduced SFAIRP.

(c) Compliance & conformance to standards, requirements, laws & legislation.

(d) The system is fit for purpose and safe to use, operate, and maintain.

The assurance strategy should use the following steps to enable progressive assurance:

(a) Determine what the system shall achieve in terms of function and performance.

(b) Define what is critical on the project in terms of its impact on systems assurance (including interfaces).

(c) Define what assurance activities are required to achieve the overall assurance goals.

(d) Conduct the assurance activities over the lifecycle of the project and progressively build assurance evidence prior to each lifecycle gateway.

(e) The summation of each lifecycle gateway assurance evidence should enable the project to present a positive assurance argument demonstrating overall assurance goals are met by the system.

4.2 Verification and validation activities

4.2.1 Design assurance strategy

The assurance strategy should identify verification and validation (V&V) activities required for system integration that will be carried out to mitigate risks identified from the interface analysis and safety in design activities outlined in Clauses 3.1.2.2 and 3.6 respectively. The strategy should outline the scope of activities and define specific functional and performance criteria necessary to verifying or validating the system and its interfaces. verification and validation activities may include, but not limited to:

(a) audits;

(b) monitoring / inspections;

(c) investigations;

(d) data capture / trend analysis;

(e) design verification and validation activities.

4.2.2 Design verification and validation

The V&V strategy shall detail the necessary strategy for progressively validating that the design will fulfil the system requirements. The strategy for progressively validating the design should include the following stage gate reviews:

(a) CDR: Concept design review – To be performed once a concept design has been formed, assessing the conformance of the concept design against its allocated system or sub-system requirements.

(b) DDR: Detailed design review – To be performed once a detailed design has been formed, assessing the conformance of the detailed design against its allocated system or sub-system requirements.

Stage gates are a mechanism for controlling progress through the project lifecycle. They provide authority to proceed to the next project lifecycle stage and are primarily an assurance surveillance mechanism. The outputs from the progressive assurance mechanisms at the system and sub-system level shall be used as input evidence for the stage gate reviews.

4.2.3 System integration and validation activities

The V&V strategy shall detail the necessary strategy for testing & commissioning stages that enable the progressive testing of system elements throughout the latter stages of the system lifecycle (design through to handover / acceptance) to assure that the system elements being implemented integrate as specified by requirements. It is recommended that the testing & commissioning activities should use the following levels of abstraction when testing or collecting assurance evidence:

(a) Level 0 – Design integration testing – Testing that the system designs integrate as specified. This could be carried out for example as a factory acceptance test (FAT) or site performance testing during construction/implementation.

(b) Level 1 – Sub-system testing (stand-alone) – Focussed testing on an individual sub-system's internal and external interfaces to determine whether they perform as

specified. This could be carried out for example as analysis of installation certification to show compliance with designs and standards.

(c) Level 2 – Sub-system Integration testing (system internal interfaces) – Ensuring that groups of sub-systems integrate as specified to enable system level performance and/or functionality. For example, this could focus on the integration of mechanical and electrical sub-systems by testing the enable functions as specified.

(d) Level 3 – System integration testing (system external interfaces) – Testing the integration of the system being developed with other systems that it interfaces with. It shall determine that the system is performing as specified within the system ICDs.

(e) Level 4 – System integration testing (operational acceptance/readiness) – Focussing on the integration of the system with the operator's people & systems

4.3 Failure analysis and monitoring

The responsible organisation shall apply failure reporting analysis and corrective action systems (FRACAS) or the equivalent during the system lifecycle. Such systems shall be used to document defects and remedial actions conducted in relation to any system interfaces during integration activities.

A record of all failure and corrective actions conducted in relation to all system interfaces shall be provided to relevant regulatory authority or adjacent system suppliers in accordance with the agreed contractual arrangements.

5 System integration reporting and deliverables

Prior to commencing system integration activities, interfaces shall be defined and categorised using the processes described in Clause 3.1.2.1. Interfaces shall be recorded in the appropriate register for use as an input to the integration activity. The following records and deliverables may be applied or produced by the system integration process:

(a) Package integration plans – developed by the interface and integration team.

(b) Interface definition sheets (IDSs) and interface control documents (ICDs) – developed by the relevant supplier system integration organisation and managed in accordance with the relevant integration strategy.

(c) Construction procedures and inspection and test plans (ITPs) – developed by the design and construction teams, compiled for the system-of-interest by the system integration organisation.

(d) Construction records and as-built records – produced by the relevant construction team and including notification of any design changes or non-conformances.

(e) Operational readiness documentation.

(f) System integration audit plans and reports.

All records and deliverables are managed in accordance with the applicable quality management system.

Appendix A Typical integration risks and mitigations

A.1 Typical risks

Below is a table of typical risks[2] that apply to complex systems integration. These cross-reference to their mitigations, shown in Section A.2.

Identifier	Complex system integration risk	Typical causes	Mitigations (TBD)
	Specification / Scope risks		
R-S1	Contracting agency has poorly or ambiguously defined the scope or badly packaged it.		
R-S2	Contracting agency has not ensured that the scope/packages and their requirements align to the project objectives.	Lack of expertise, peer review or stakeholder buy-in, poor requirements management, allowing requirement to be included without assessing or clarifying their rationale, "gold plating".	
R-S3	Under and/or over specification of work.	The detail or reach of the requirements is not appropriate or unnecessarily constraining. Under specification can be the cause of limited time, expertise, motivation or peer review. Over specification can be caused by pet-projects creeping in, lessons badly learnt, lack of experience (by contrast to book knowledge) or peer review.	
R-S4	Scope increases, opportunistic works or late breaking changes that undermine the ability to deliver the plan.		
	Adaptation risks		
R-A1	The contracting agency underestimates the amount of product adaptation or development to meet their requirements.		
R-A2	The supplier underestimates the application environment.		

[2] Derived from http://www.irse.org/knowledge/publicdocuments/ITC%20Report%2057.pdf and XXX

Identifier	Complex system integration risk	Typical causes	Mitigations (TBD)
R-A3	The supplier finds that they overestimated their ability to adapt the product to meet the requirements.		
	Specific integration risks		
R-I1	Interfaces are not well developed, defined, designed or tested, prior to integration.		
R-I2	Interfaces between contracting parties are not developed or are underestimated.		
R-I3	Contracting Agency does not take leading role in specifying and managing interfaces; or does not check that the interfaces will support the overall objectives.	Sys Integrator role is not fulfilled or not assigned to a capable party. Parties cannot gain access to information (from each other or regarding installation environment, via CA).	
R-I4	Information regarding interfaces does not exist, is not available, is outdated, or is poorly developed. As such, interfaces are not well implemented and/or integration issues cannot be resolved in a timely manner.	This could be due to commercial issues, contracting agency or supplier capability, data management, legacy installations etc.	
	Design risks		
R-D1	Designs and details designs that are not (fully) aligned to the requirements or interfaces.	Supplier selection, or supplier competence. Poor engineering management. Last minute changes. Poorly written specifications.	
R-D2	Too many assumptions made by the designer.	Lack of communication or time to review assumptions between contracting agency and suppliers, or between suppliers.	
	Migration, commissioning and operational readiness risks		
R-M1	Optimistic or unrealistic migration plan and implementation schedule.		
R-M2	Optimistic or unrealistic view of track access constraints.		

Identifier	Complex system integration risk	Typical causes	Mitigations (TBD)
R-M3	Optimistic or unrealistic view of external dependencies.	Poor stakeholder engagement and review. System boundaries not understood, and so not taken into account effectively.	
R-M4	Poor logistics planning or implementation.		
R-M5	Suppliers needs are not considered during migration planning.	Supplier does not understand them / communicate them. Contracting Agency does not receive them (or ask for them) with enough time to implement them. CA does not understand the supplier's requirements. CA does not prioritise and balance the needs between suppliers or communicate the plan (and it's limitations/exclusions) in advance, or in enough detail.	
R-M6	Migration plan or implementation schedule do not provide enough contingency with respect to passenger service requirements/deadlines.		
R-M7	Contracting Agency does not articulate the operational business' needs; allowing suppliers to make ambitious assumptions.	Operational, maintenance or business-as-usual activities are not taken into account.	
R-M8	Responsibilities are flowed down to suppliers that they are not best placed to manage, especially where a close relationship to the operational is required.	Contracting Agency assigns full responsibility for implementation of operational equipment to supplier; or a method of managing those specific risks is not included in the scope of work.	
	Safety certification risks		
R-C1	The level of work required to achieve safety certification of the products is underestimated.	Primarily the responsibility of the supplier, and thus mitigated by their competence and approach; but a positive and mature approach can be led by the contracting agency and specified or influenced in the scope of works. The approach to the method of work during execution, or the lack of collaboration of the contracting agency.	

Identifier	Complex system integration risk	Typical causes	Mitigations (TBD)
R-C2	The level of work required to achieve safety certification of the System is underestimated.	The System boundary is not well defined or understood, thus activities are not identified or allocated. The CA does not recognise its obligations for achieving (or at least assigning and supporting) safety for the emergent properties of the system.	
R-C3	The contracting agency does not manage the safety certification of those elements of the project that are external to any suppliers' scope, such as external interfaces and operating and maintenance readiness.		
	System availability/Reliability risks		
R-R1	Failure to achieve and sustain an acceptable level of product reliability/availability when the product/System is cut-over into revenue service.	Inadequate or incomplete product test & commissioning, or insufficient attention to maintainability and maintenance training (which is typically a joint supplier/contracting agency responsibility).	
R-R2	Failure to achieve and sustain an acceptable level of System reliability/availability when the System is cut-over into revenue service.	Inadequate or incomplete system test & commissioning, or insufficient attention to maintainability and maintenance training (which is typically a joint supplier/contracting agency responsibility).	
	Stakeholder engagement risks		
R-E1	The project does not take into account critical details to implementation including, but not limited to, maintenance, operational, training, logistic, political, commercial, sponsorship or other contextual needs.	Stakeholders are not identified early enough, or not engaged with effectively or in a timely manner for the project to implement their needs or gain buy-in and acceptance in time.	
R-E2	**Capability alignment risks**		
R-E3	The complexity of the project was underestimated.	Performance, functionality, physical scale, environmental interfaces, regulatory requirements or operational needs were not all taken into account.	

Identifier	Complex system integration risk	Typical causes	Mitigations (TBD)
R-E4	Supplier unable to mitigate or manage risks passed to them.	Misalignment of risks passed to supplier and the supplier's capability; or failure to provide the supplier with the support (material, communication, time, access to other parties) required to manage the risks.	
R-E5	Misalignment of the scope, cost and time of the project.	Failure to recognise the limiting factor and work within those constraints (overly ambitious deadlines / scope complexity, or optimistic budgets). The boundaries of the System were not identified or developed sufficiently.	
R-E6	Misalignment of product capability with project planning.	For example, failure to base the migration boundary on the signalling system capability; or failure to prepare the railway for new Rolling Stock EMC characteristics.	
R-E7	Migration phases overrun or are not achieved.	Migration regions are too large or contain too much complexity.	
R-E6	Misalignment of product capability with project planning.	For example, failure to base the migration boundary on the signalling system capability; or failure to prepare the railway for new Rolling Stock EMC characteristics.	
R-E7	Migration phases overrun or are not achieved.	Migration regions are too large or contain too much complexity.	

A.2 Mitigations

Below is a table of mitigations, each of which address one or more of the typical risks (section A.1). These mitigations are referenced throughout the standard to demonstrate what the clauses will help to achieve, and why. Understanding the rationale may, where necessary, allow the project team to implement alternative strategies.

Identifier	Mitigations	Rationale
M.1	**Use systems engineering** Determine the system engineering activities required throughout the project (see?? guidance in this standard?) and ensure that they are assigned to a party (the [prime] system Integrator) with the capability to undertake them.	System engineering covers all early and late phase activities, including system integration. System engineering is a mature approach to mitigating system integration risks. Depending on the nature of the works, only some of the techniques may be required - but this should be determined through effective analysis at the initiation of the project and communicated to all affected parties. Some of these techniques are referenced as mitigations below, if the risks are not likely to impact the project, then implementing the mitigation may not be necessary.
M.2	**Implement a design management process** Embedded into the scope of works and understood by all parties.	Ensures traceability between designs, requirements (project objectives) and interfaces agreed across the project; which is then used to verify that designs implement and align to the requirements and interfaces, and thus that they are in accordance with expectations of all parties.
M.3	**Implement stage/phase reviews with gates** Define or implement a lifecycle for the project, based on the project's characteristics. Specify any planned iteration (e.g. migration stages) and allow for iteration for unforeseen changes or issues. Define pass criteria for the gates at the outset of the project. The pass criteria should reduce risks on the project to an appropriate level for each gate's timing in the overall lifecycle. Ensure a rigorous gate process is followed, with independence where necessary, and that all material is complete, available and reviewed before a gate is held.	Stage gates ensure that the maturity of the overall works has reached an appropriate level of maturity to avoid carrying unnecessary risks into the following activities, and before any increased level of investment occurs (e.g. implementation, procurement or deployment). Defining pass criteria in advance allows parties to prepare themselves and increase the chance of success of the gate.
M.4	**Configuration and version control** Establish the relationship between documents (document hierarchy), designs, schedules and other artefacts. Ensure that all work is versioned uniquely and identifies with specific versions of upward documents in the hierarchy. Ensure that changes are applied to specific versions of documents, and that change impacts look at all related works (using the	It should be possible to ascertain the inputs that an output is derived from (e.g. a schedule for a specific version of a scope of works). This also allows for easier impact analysis when changes are made, as related documents (and their derivates) can be easily identified and updated (or at least marked "at risk"). Once the project is in full-swing, the ability to quickly identify impacted works, and as such scope the changes and implement them. For example, changing a product

Identifier	Mitigations	Rationale
	hierarchy, as appropriate). Identify a point at which change control comes into force, and at that point establish a change control board, representing all impacted stakeholders, to review and authorise changes.	due to a failed test, before putting that change into service, along with all the supporting material (training, safety certification, limitations etc.). The change control board ensures that the impact of changes is widely reviewed by appropriate authorities or impacted parties. The Table of risks highlights the importance of peer review.
M.5	**Broadcast the project baseline** Ensure that the baseline (specific versions of related documents) that the project is working to is known by all parties.	Sometime this is implemented using a single set of tools and data (e.g. BIM or DOORS Next Generation) but real time access to working material poses its own risks. Clarity on current versions and working to specific versions of a document achieve this mitigation, which could also be done through good collaboration and communication.
M.6	**Manage stakeholders** Identify stakeholders at the beginning and periodically through the project. Identify any specific needs or constraints they have (e.g. fixed sitting dates for panels). Determine appropriate frequencies of engagement for each one, along with the materials and ideal outcomes/project dependencies for each engagement. Determine events that would trigger ad-hoc engagements. Build a stakeholder management plan on this basis and ensure that it is incorporated into the project implementation schedule, with risk/contingency as necessary. Applies from the beginning of the project until completion.	Understanding the project's stakeholders and how the project should engage with them to achieve their goals means that this can be planned for, and reduce (but not eliminate) the probability of late changes. It can be that certain groups hold expert knowledge that is not otherwise documented or known to the project team (for example users and their representatives, political actors, funding or regulatory bodies). In other cases, gaining early buy-in to the project's plans can be beneficial to avoid delays at project migration stages or acceptance. It also helps to elicit any specific requirements they may have but would not have considered before seeing the project's work.
M.7	**Manage issues** Maintain a register of system issues that identify areas of technical concern or non-compliance, in addition to the usual project management controls. Allow suppliers to promote issues to the register, where they feel their products/services can affect other parties. Establish and execute mechanisms for sentencing the issues and either resolving them or gaining acceptance with the end user such that this is well-rehearsed before initiating any work that impacts the operational services.	Enables issues to be identified, understood and resolved. Especially enables those late in the process, or during test/commissioning, to be quickly escalated in a coherent way, understood the same way by all parties and therefore addressed in a controlled manner with minimal confusion/interpretation. This, combined with configuration and version control, should lead to agile resolution to real-time problems that can (will) crop up during system Integration.
M.8	**Scope development activities**	Development requires management, interpretation and has inherent risk. Use of items already proven to solve a problem, especially if battle-tested, means that the integration problems have been resolved elsewhere where they are not unique to

Identifier	Mitigations	Rationale
	Use of standards-compliant or COTS subsystems to meet the requirements, where possible. Gain a supplier view of the technology readiness levels, or other metrics of product maturity, of components as early as possible. Review this at each stage gate for any changes. Ensure that these metrics drive the risk allocation to development, testing and commissioning and integration activities.	the project. Knowledge/expertise on the interface is also more widespread, leading to faster resolution of any issues. Use of industry-accepted metrics to gauge development and integration risks will provide an evidence-based approach to the risks being undertaken. See http://space4rail.esa.int/technology-readiness-levels-trls for more information.
M.9	**Scope maturity across the system** Use interface maturity levels (IMLs), starting at the system conception phase, and progressively manage those through to delivery. Ensure that low maturity interfaces have specific controls/processes in place to manage their development, testing and introduction.	Ensures that identification of high-risk interfaces is performed early, and therefore the overall team apply the necessary effort and time to manage low risk interfaces in a controlled way. Enables identification, e.g. of those interfaces most in-need of off-site or early simulation/modelling/prototyping etc. Mapping the maturity of interfaces between products (or suppliers) will help to determine the risk across the whole system. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA507276
M.10	**Visualise, prototype, and test early and off site** Perform early and off-site testing. Invest in prototyping, integration rigs at subsystem and system levels, covering as much testing as possible before integration in a methodical manner. Repeat tests where design or implementation changes occur. This identifies interface issues before they occur. Scope the tests / Determine the outcomes that a supplier cannot perform/prove on their own and put specific activities in place for these.	Early identification of issues can decrease rectification costs by orders of magnitude. Prototyping, before a system has been implemented, helps engineers to see new sides to the problem and helps users (and other stakeholders) visualise the engineering plans; as such each party can identify problems before it's too costly to change them. The same applies to all levels of implementation, testing and integration, and as such consideration should be given to the benefits of modelling, prototyping or early integration testing; particularly of complex areas or areas of development. Even if the whole project scope has been broken down and assigned entirely to other suppliers, it does not mean that these suppliers can demonstrate that the whole project scope has been delivered. This is especially true of emergent properties and functional properties that rely on interfaces. *If a top level requirement asks that a passenger can make a journey, it does not necessarily mean that a train, some signalling and some information will allow passengers to make journeys - and the suppliers will not test for this (they'll test their products according to their scope of works). The system Integrator shall ensure that "making a journey" has tests designed specifically for it, once all the other pieces are in place.*
M.11	Encourage subsystems/suppliers who work on any specific interface to use the same language, reference points, models etc.	

Identifier	Mitigations	Rationale
M.12	Ensure that the project is clear on its system scope and interfaces, and that these are agreed by all parties and supply chain.	
M.13	Ensure that the project is clear on how the subsystems that make up the system interact. Commercial, engineering and project management to be on the same page regarding the makeup of the sub-system elements (whether that's axles for a train, or stations for a railway).	
M.14	Ensure that the project team design/planning accounts for functionality across the system (e.g. "move passengers" at the top level, e.g. "keep time" at the bottom). Test for those functions progressively before introduction rather than relying on integration being successful through subsystem design.	
M.15	Ensure the project team is clear on their own scope / the risks only they can manage. This is likely to start with any issues that span sub-systems / suppliers. If a supplier/subsystem team is asks to manage a risk on your behalf, ensure they have the tools, rights and capability to do so; including to speak to and influence the parties involved.	

Appendix B Bibliography

The following referenced documents are used by this Standard for information only:

- ASA T MU AM 06014 GU - Guide to Systems Integration
- INCOSE - Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities

Appendix C Hazard register

Hazard number	Hazard	Heading number(s)
5.0 Rolling Stock	All the hazards associated with rolling stock identified in the RISSB hazard register.	
6.0 Infrastructure	All the hazards associated with infrastructure identified.	
8.0 Operations	All the hazards associated with operations identified in the RISSB hazard register	
9.0 Signals Infrastructure	All the hazards associated with signals infrastructure identified in RISSB hazard register.	
10.0 Degraded Working	All the hazards associated with degraded working identified in RISSB hazard register.	

About Rail Industry Safety and Standards Board

The Rail Industry Safety and Standards Board is a not for profit company limited by guarantee. Wholly owned by its funding members, RISSB is required to apply the whole of its income and assets to achieving the objects listed in its constitution.

RISSB is responsible for the development and management of Standards, Rules, Codes of Practice and Guidelines for the Australian rail industry.

For further information, visit www.rissb.com.au

RISSB Australian Standards Development Process

The Standards development process is rigorous and transparent.

Authors work with RISSB's Standards Development Managers and Development Groups to ensure that products are acceptable to industry. Standing Committees oversee this work and ensure that proper governance and process is followed. The products are exposed to the public and industry for comment and validated by an independent validator.

Once agreed by the Development Groups, Standing Committees and Validator, the drafts are passed to the RISSB Board for approval.

The same process is used in developing other RISSB products, although Guidelines are not exposed to the public for comment or validated, given their non-binding nature.

Standards Development and Accreditation Committee

RISSB is accredited by the Standards Development and Accreditation Committee (SDAC), and all Standards produced by RISSB since 31 July 2007 are published as Australian Standards.

The Standards Development and Accreditation Committee audits RISSB annually to ensure that RISSB's processes are in accordance with SDAC accreditation requirements.

Sales and distribution

Australian Standards developed by RISSB are sold and marketed through SAI Global. For further information, please visit www.saiglobal.com.

Financial members of RISSB are granted access with membership.

RISSB
RAIL INDUSTRY SAFETY AND STANDARDS BOARD

ABN 58 105 001 465

For information regarding the development of Australian Standards developed by RISSB contact:

Rail Industry Safety and Standards Board

Brisbane Office
Level 4, 15 Astor Terrace
Brisbane, QLD, 4000

Melbourne Office
Level 4, 580 Collins Street,
Melbourne, Vic 3000

PO Box 518
Spring Hill, QLD, 4004

T +61 7 3274 000
E Info@rissb.com.au

For information regarding the sale and distribution of Australian Standards developed by RISSB contact:

SAI Global Limited
Phone: 13 12 42
Fax: 1300 65 49 49
Email: sales@saiglobal.com
http://infostore.saiglobal.com/store

ISBN: Enter ISBN.