A Systems Approach to Safe System Integration in Major Rail Projects

R. Kusumo
Technical Division
The Office of National Rail Safety Regulator
PO Box 3461, Rundle Mall, Adelaide SA 5000, Australia

Abstract

The safety of modern railways relies on various interdependent systems that operate seamlessly together forming a system of systems in the rail network. Major rail projects are usually complex and have significant impact on a railway's safety, as they usually involve implementing, changing and integrating a number of new railway systems, as well as integrating with existing systems in the rail network.

Given the increasing complexity of railway systems, the integration of a system with new or legacy systems may cause unintended behaviour of any of the systems, as well as the whole integrated system. As such, the traditional approach to delivering major rail projects where each railway system is designed, implemented and tested in isolation of other interconnected systems is no longer sufficient to ensure that the rail network can be operated safely.

A systems approach to implementing change in the railways, especially in integrating multiple new or legacy rail systems is required to ensure that the railway's operations remain safe, so far as is reasonably practicable. This approach needs to cover the system life cycle: including requirements analysis, system design, system implementation, testing and commissioning, service operation and maintenance, as well as decommissioning.

This paper presents a case study of a typical major railway project in Australia demonstrating how designers, system integrators and rail transport operators can adopt a system approach to safely integrate complex rail systems that meets the requirements of the Australian *Rail Safety National Law*.

Introduction

The complexity of railway safety systems can be seen in the variety of technologies and the number of suppliers that contribute to the subsystems that collectively provide safe railway operations. This complexity is further compounded as it is not just limited to new subsystems: in the railway environment it will normally also include integrating new systems with older, existing, systems. This is particularly evident in major projects involving new rolling stock or the provision of signalling, communication and control upgrades.

Notwithstanding the complexity of integrating multiple systems in a rail network, the *Rail Safety National Law* (RSNL) does not contain any sections that are specific to system integration. Nonetheless, the RSNL contains the following sections that require all relevant parties (designers, manufacturers, suppliers, installers, commissioning personnel and the rail transport operators (RTO)) to manage safety risks on the railways, including risks that are associated with system integration:

- Section 46 – *Management of risks*: The designers, contractors and RTOs need to eliminate safety risks associated with system integration or minimise them so far as is reasonably practicable (SFAIRP);
- Section 52 – *Duties of rail transport operators*: The RTO has to ensure to its satisfaction that the integrated system is safe SFAIRP for its railway operations; and
- Section 53 – *Duties of designers, manufacturers, suppliers etc.*: The designers, manufacturers, suppliers, installers and commissioning personnel have to ensure that the system and subsystems are safe SFAIRP for their intended use on the railway.

In addition to the above RSNL sections, Schedule 1 of the RSNL Regulations requires the RTO to have the following procedures as part of its Safety Management System (SMS) to manage change to railway systems:

- Clause 12 – *Management of change*: The RTO needs to have procedures to manage change on the railway safely SFAIRP;
- Clause 19 – *General engineering and operational systems safety requirements*: The RTO needs to have procedures to control and verify the integrated systems in accordance with operational system safety standards; and
- Clause 20(1) – *Process Control*: The RTO needs to have procedures to test safety related engineering and operational systems.

A robust approach to systems integration is essential for major projects that are delivering complex and multiple safety systems; one that allows the project to manage the increasing complexity of railway systems integration and to meet its safety duty that is stipulated in the RSNL.

A System Approach to Complex System Integration

A system is defined as an assemblage or combination of elements or parts forming a complex or unitary whole. These system elements are interrelated and work together towards a common goal. The interrelation and synergy between elements facilitate the work of transforming inputs into outputs [1]. A diagrammatic representation of a generalised conception of a system as formulated by Flood and Jackson [2] is shown in Figure 1.

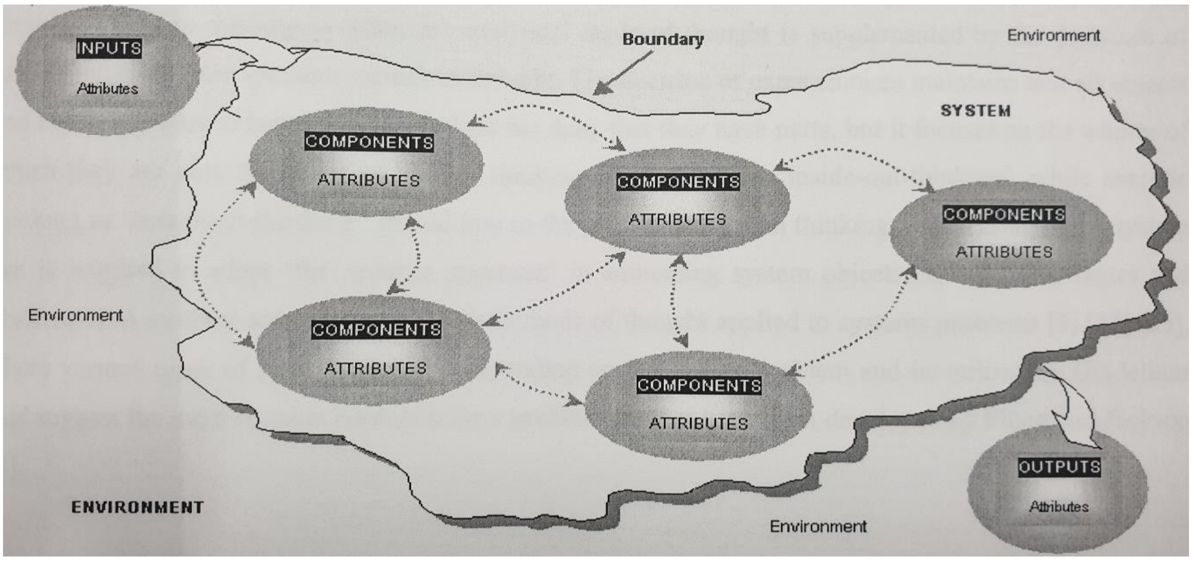

Figure 1: A general conception of a system

A system approach to safely integrate complex rail systems initially involves determining and analysing the interrelationships between system elements that form the system structure. For example, a typical train radio system (TRS) for voice communication may consist of a series of interrelating subsystems forming a system of systems. A high level TRS system structure may consist of the following subsystems:

- User machine interface (UMI) that allows the train controller/signaller to transmit and receive voice communication using the TRS network.
- Communication Server that processes and transmits voice communication from UMI to base stations.
- Base stations that include the antenna, radio tower and communication equipment to relay the signals across the rail network.
- On-board equipment that comprises antenna and equipment to transmit and receive voice communication to and from the train.
- Driver machine interface (DMI) that allows the train driver to transmit and receive voice communication using the TRS network.
- To operate in a rail tunnel, the TRS subsystems may also include antenna (e.g. leaky coax antenna) and fibre optic cable to transmit the communication signal in the tunnel.
- Handheld communication equipment to allow track worker crew to transmit and receive voice communication using the TRS network.

Figure 2 presents the high level view of a typical TRS system structure.

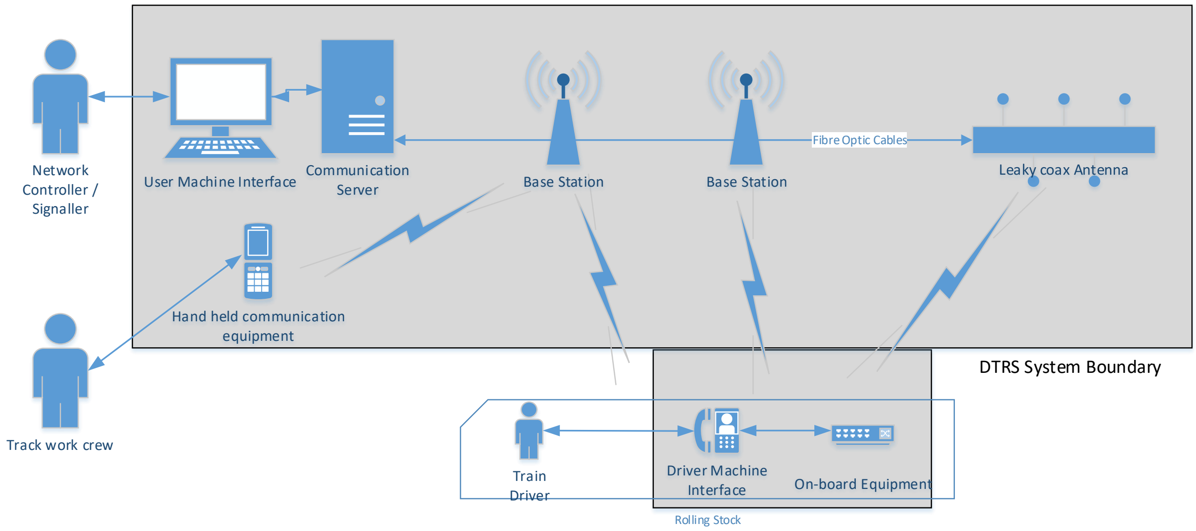

Figure 2: High level view of train radio system structure

A railway system generally follows a typically system lifecycle. An example of a system lifecycle is illustrated in Figure 3. For a major rail project, the activities to ensure safe system integration commence at the beginning of the system lifecycle (requirement analysis phase) and progress through to the operations and maintenance phase. To be satisfied that new technology is being delivered with its component parts safely integrated and that the system as a whole is safely integrated with existing assets, the system integration project needs to adopt a system approach at each stage of the system lifecycle. This approach will allow the project to specify, design, install and test the interfaces and interdependencies between multiple systems in the rail network.

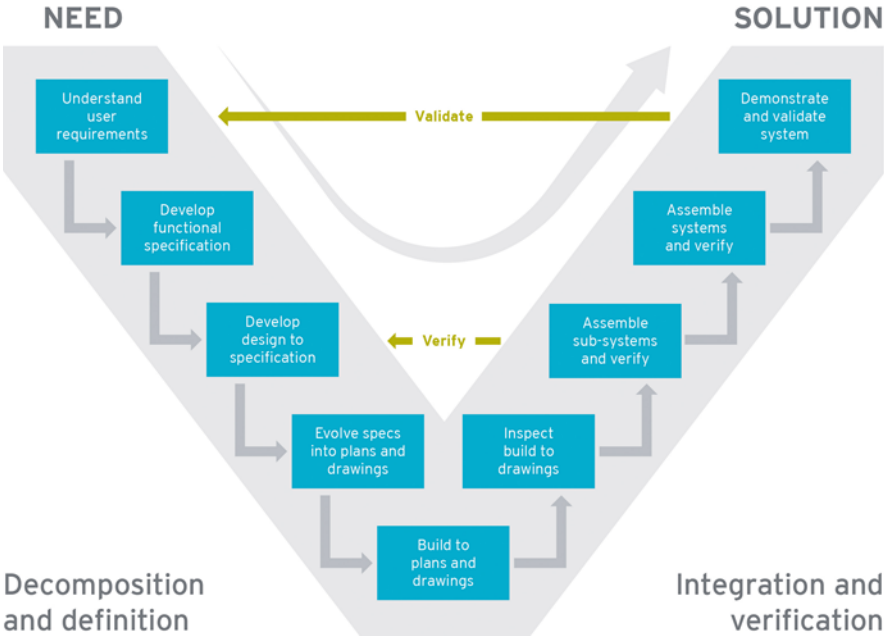
NEED
SOLUTION
Understand user requirements
Develop functional specification
Develop design to specification
Evolve specs into plans and drawings
Build to plans and drawings
Inspect build to drawings
Assemble sub-systems and verify
Assemble systems and verify
Demonstrate and validate system
Validate
Verify
Decomposition and definition
Integration and verification

Figure 3: V-Model of a typical system cycle

The safe integration of a TRS on an existing rail network would require the establishment of the system lifecycle. Throughout each phase of the system lifecycle, the implementation of TRS will need to consider not only how the subsystems will be integrated, but also how these subsystems will interface with the following systems that are outside TRS system boundary:

- Existing railway infrastructure, for example how the TRS base stations will be connected to the local power supply;
- Different types of rolling stock, for example how the TRS on-board equipment will be connected the train power supply; and
- Different types of user, for example, how the network controllers, train drivers, signallers interact with the UMI and DMI.

Requirement specification phase

A system lifecycle usually commences at the requirement specification phase [3], which involves analysing how a new system can be operated and maintained in the rail network. The output of this phase is the establishment of the System Requirements Specification (SRS) for the new railway system. To ensure safe integration, the SRS for a system needs to consider the interface requirements between it and any subsystems and between it and any existing or legacy systems. In addition, these interface requirements for the new system need to include any Safety Related Application Conditions (SRACs) on the existing railway systems that will impact the new system.

Following on with the TRS example, a project would need to determine the SRS for TRS which may include the following types of requirements:

- *Functional requirements*: An example of TRS functional requirements may include how the system will manage emergency calls to ensure safe railways operation;

- *Operational requirements*: An example of TRS operational requirements may include how the train driver can interact with the DMI whilst safely operating the train;
- *Physical requirement*s: Examples of TRS physical requirements may include the DMI position in the driver's cab to ensure safe train operation, and the connection of TRS base stations with the local power supply; and
- *Safety Related Application Conditions (SRACs)*: An example of an SRAC that can apply to TRS may include the electromagnetic emission from the system that can interfere with an existing signalling system.

Design phase

The safety of a railway system is governed by how its design can achieve its SRS [3]. A system approach to designing railway systems that will ensure safe system integration involves a systematic analysis of the following:

- Interface compatibility between connected railways systems (data, power and signal, etc.);
- Risks associated with failures of interface between interconnected systems;
- Risks of system failure which may compromise the overall safety of the railway operations;
- Compliance with Safety Related Application Conditions (SRACs) from any existing or legacy systems; and
- Verification that the identified risk controls have been incorporated in the system design.

To illustrate the application of system approach in the design phase, a typical TRS design will need to consider the following aspects to ensure that it can be safely integrated into the rail network:

- TRS interface compatibility analysis, such as the compatibility of power that is being supplied by batteries on the rolling stock and the TRS on-board equipment and DMI;
- TRS interface hazard analysis (IHA), such as hazards associated with potential TRS UMI interference with other train communication systems operated by the network controller;
- TRS system hazard analysis (SHA), such as hazards associated with TRS DMI failure to alert the train driver of emergency calls; and
- TRS compliance with existing SRACs on the rail network, such as TRS compliance with a restriction on electromagnetic emission that may interfere with existing signalling systems.
- TRS risk controls verification, such as ensuring that the TRS base station designs have incorporated appropriate alarms to monitor the status of uninterrupted power supplies and mitigated against risks of TRS failure due to power outage.

Installation/construction phase

How a railway system is installed can have a significant impact on its safe integration on the rail network. Any errors in installing and configuring the system, especially the system interface elements (e.g. data communication ports, power cables connection, etc.) can result in a wrong side failure of other interconnected safety critical systems. As such, it is vital that system interface and identified risks controls are verified for correct implementation and conformance with the system design during the installation phase. If there are any deviations in implementing the system interface and risk controls from the approved design, then the safety impact of these deviations will need to be assessed to ensure that the associated risks are eliminated or mitigated SFAIRP.

For example, any errors or deviation from system design in setting the TRS DMU and UMI to display and sound emergency calls may result in the train driver, network controller or signaller missing an emergency call, with very serious consequences.

System testing phase

Prior to integrating a railway system into the rail network, the system needs to be fully tested as a standalone system to ensure that its safety functions can operate correctly and has met the specified requirements. These tests are often conducted as part of Factory Acceptance Test (FAT) and Site Acceptance Test (SAT) for the system.

To ensure that the system can be integrated safely into the rail network, the testing of the standalone system needs to consider how the system will eventually interact with other systems in the rail network.

For example, the testing activities to implement a TRS may involve examining the system safety functions by providing different types of inputs from other interfacing systems, including legacy systems. The results of safety testing will help the RTO to ensure that the TRS, as a standalone system, can achieve the following:

- Safely receive the inputs provided by the interfacing subsystems (e.g. emergency voice communication can be clearly transmitted from multiple base stations);
- Safety functions are not compromised due to inputs from other subsystems (e.g. failure of local power supply will not inhibit TRS functions to transmit emergency calls);
- Safely generate the required outputs to the interfacing subsystems (e.g. emergency voice communication between network controller and train drivers can be transmitted clearly without delay); and
- Generated outputs will not compromise the safety of the interfacing subsystems (e.g. TRS will not interfere with the signalling systems and rolling stock systems).

System integration phase

Complex railway systems will usually undergo a multitude of tests when they are integrated into the railway to verify and validate the system functionalities. From a system safety perspective, a safety verification and validation (V&V) process is key to the systems integration as it ensures that multiple safety systems function together in a manner that assures the safety of railway operations as a whole.

Safety verification aims to determine, for a particular project lifecycle phase, that the safety requirements for that phase are fulfilled with respect to completeness, correctness and consistency. The results of the safety verification process determine that the “safety related system is built right”.

Safety validation aims to demonstrate that the system safety functions, before and after system installation and integration, meet the safety requirements. The results of the safety validation process determine that the “right safety system is built”.

A system approach to conducting safety V&V involves systematically testing the effect of one subsystem on another subsystem. Consequently, the changes in the behaviour of both the subsystems and the whole integrated system can be examined when the systems are all combined together.

The safety V&V for implementing a TRS system may involve operating the system along a specific rail corridor to determine if:

- it is still functioning correctly (e.g. can TRS transmit voice communication clearly); and
- its function can meet the operational requirements (e.g. can TRS transmit voice communication within a specific time delay).

The results of safety V&V will help the RTO to ensure that with the integration of a TRS, the rail network can achieve the following:

- Functions of other safety critical systems are not compromised after the TRS is integrated into the rail network (e.g. TRS is not emitting electromagnetic interference that may affect the signalling system functions in the rail network);
- Safety risks associated with TRS integration and testing activities, particularly risks associated with interfaces with other railway systems, have been eliminated or mitigated SFAIRP (e.g. testing of TRS on the rail network will not result in trains passing signals at danger due to train diver confusion); and
- TRS, as an integrated system, has met the specified functional and operational safety requirements (e.g. TRS is able to clearly transmit emergency calls for a specific location in the rail network without significant delay).

Operation and maintenance phase

A railway system should be ready to commence operation and maintenance (O&M) in the rail network after completing its testing regime. A system approach to ensure safe O&M of the integrated system involves the RTO continuously monitoring the following:

- All faults and corrective actions that were identified during the testing phase have been addressed;
- All residual risks associated with the railway system are within acceptable limits;
- All the system SRACs that were identified during safety V&V have been implemented when operating and maintaining the integrated systems; and
- Any failures identified when operating and maintaining the integrated system are managed safe SFAIRP.

From the TRS example above, to safely operate and maintain the system post-integration into the rail network, the RTO needs to monitor the following:

- Operational TRS faults, such as connectivity with other train communication systems for network controller to driver communication;
- Effectiveness of controls to manage TRS residual risks such as driver training to mitigate human factor risks associated with train driver operation;
- TRS SRACs such as conditions associated with base station power supply monitoring, alarm and response; and
- TRS faults that are identified during system operating such as signal dropout rates, especially at potential blackspot areas across the rail network.

Case Study

This section of the paper presents a case study on a typical major rail project in Australia that involves integrating a TRS into a metropolitan rail network. The case study discusses the challenges that the project encountered during system integration which ultimately caused delay in its ability to demonstrate that the system was safe SFAIRP for the intended railways operation.

Train Radio System (TRS) implementation in a metropolitan rail network

A RTO had a project to implement a new TRS system across a metropolitan rail network. The TRS was originally designed, installed and tested using base stations. The initial test showed that the radio signal can be communicated with an acceptable time delay to ensure safe railway operations. The TRS was developed to SIL 0 according to CENELEC Standards [3],[4],[5] and integrated into multiple rail corridors and multiple types of rolling stock.

During the initial system integration, the TRS showed a significantly higher time delay in communicating the signal, which was outside the safe operating requirements. This communication delay was due to the communications network relying on a series of base stations rather than operating from a single base station. As such, the internal TRS software needed to determine the signal strength from multiple base stations, rather than just one.

Consequently, to reduce communication delay, the TRS software had to be modified to limit the search to signal strength from only the closest base stations. The modified software then underwent system integration testing (SIT) on each rail corridor and each type of rolling stock. This SIT regime aimed to ensure the following:

- Geographical specific issues in the rail corridors (e.g. potential black spots and interference sources) would not affect the TRS availability (including communication delay) and reliability.
- Rolling stock specific issues (e.g. interference sources and DMI design) would not affect the TRS system performance (e.g. audio clarity) and train driver's ability to safely use the TRS.

Given the faults and subsequent modification completed during the SIT that could affect safe operation of the system, the RTO had to complete additional risk assessments and system retesting. These additional safety assurance activities generated further evidence that was provided to ONRSR to demonstrate that the safety assurance strategy has been achieved to mitigate the associated safety risks SFAIRP. The evidence provided to ONRSR included the following:

- Management Plans (e.g. safety management plans, testing & commissioning plans) that specified the strategy to ensure the system was designed, installed, tested and commissioned safely.
- Risk registers.
- Independent safety assessor review.
- EN 50128 SIL 0 compliance report.
- A Safety Assurance Report (SAR) that contained the safety argument that the system was safe SFAIRP.

- Operational Readiness SAR for implementation on a single railway corridor and using a single type of rolling stock. This SAR contained the safety argument that the TRS was safe SFAIRP for the intended railway's operations, and was subsequently updated as the TRS was implemented in different rail corridors and on different types of rolling stock.

Conclusion

Integrating railways systems is complicated and may significantly impact the safety of railway operations. By adopting a system approach to integrating complex railway systems, it allows the designers, system integrators and the RTO to better understand the subsystems and system level interfaces. The project can therefore implement system functions and features that will ensure the subsystems operate seamlessly together and that the integrated system meets the safe operating requirements of the intended railway.

The case study presented in this paper showed that integrating a system could result in significant system errors if a system approach was not adopted. These system errors in turn would lead to the project having to conduct additional safety assurance activities in order to demonstrate that it has met the requirements of RSNL in managing safety risks SFAIRP.

Reference

[1] Chapman, W. L., Bahill, A.T. and Wymore, A.W. 1992, Engineering Modelling and Design, CRC Press Inc, Florida.

[2] Flood, R. L. and Jackson, M. C. 1991, Creative Problem Solving – Total Systems Intervention, John Wiley & Sons, England.

[3] I.S. EN 50126 – 1:2017, Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process.

[4] I.S. EN 50128:2011. Railway Applications – Communication, Signalling and Processing Systems – Software for Railway Control and Protection Systems.

[5] I.S. EN 50129:2003. Railway Applications – Communication, Signalling and Processing Systems – Safety Related Electronic Systems for Signalling.