ONRSR Fact Sheet

Systems Integration Fact Sheet

July 2020

Innovation and new technology can support safer railways, but challenges exist in safely introducing complex systems to railway operations.

Effective systems integration is essential to ensure that new technologies safely work together and with existing railway systems.

Why is this important for safety?

A robust approach to systems integration is essential for major projects and other undertakings that are delivering complex and multiple safety systems.

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. It will typically also include integrating new systems with older, existing systems. This is particularly evident with the introduction of new rolling stock or the provision of signalling and control upgrades.

The safety verification and validation (V&V) process is key to the systems integration approach. It ensures that multiple systems function together in a manner that assures the safety of railway operations.

The safety V&V activity commences in the design phase and progresses through to the operations and maintenance phase.

It is important to recognise that the behaviour of both the subsystems and the whole integrated system may change when they are all combined together.

As such, system integration activity needs to assure that:

> safety functions are not compromised after subsystems are integrated together

> the safety risks associated with system integration and testing, particularly at interfaces, have been mitigated so far as is reasonably practicable (SFAIRP)

> the integrated system has met the specified functional and operational safety requirements.

System safety verification and validation

In the delivery of a project, a rail transport operator (RTO) will identify safety risk controls, including controls for interface related risks, through its risk management process.

These safety risk controls need to be implemented and their success is supported by system safety V&V activities. Such activities typically commence during the design lifecycle phases and are iterated throughout construction, testing, commissioning, operation and maintenance phases of the project.

At each phase of the project lifecycle, the safety V&V activities will have different aims ranging from ensuring that risk controls are built into the design, to testing their functionality during commissioning, and monitoring their performance during operation.

Safety verification:

The activity to determine that the project lifecycle phase fulfils the requirements of that phase 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:

The activity 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".

System integration activities

An RTO has a duty to ensure that safety risks to its railway operations are managed SFAIRP. To be satisfied that complex systems are being delivered with their component parts safely integrated, both within the new systems and with existing assets, an RTO must have processes in place that plan and document safety related system integration activities.

As a foundation, planning activities should adopt good practice safety V&V. For example, using recognised standards such as:

> IEC 61508

> EN 50126 / 50128 / 50129

> AS/NZS ISO/IEC/IEEE 15288.

By preparing a safety V&V strategy based on appropriate standards, an RTO can carry out the analyses and tests that will assure safety. These should show that the safety functions of the complex system are successfully implemented at all stages of a project. Building on the safety V&V strategy, an RTO can prepare a system safety plan which should, as a minimum, include:

> the roles and responsibilities of all parties involved in safety V&V

> the safety V&V processes to be applied

> the extent of safety function testing required to assure safety

> the safety evidence to be produced.

Supporting the system safety plan, an RTO can prepare a system integration plan which should, as a minimum, include:

> the roles and responsibilities of all parties involved in system integration

> the system integration processes to be applied

> the extent of safety V&V required to assure safety, after the subsystems and system have been integrated together.

It is important that an RTO knows that its system integration activities have managed system safety risks SFAIRP. Such safety risks would include those associated with system integration activities, testing activities, and the failure of interfaces between subsystems and systems.

For an RTO to assure itself that the integrated system can safely enter into service, it should document both system safety and system integration activities. This would typically include evidence that:

> all system interfaces have been identified and interface related safety risks have been eliminated or mitigated SFAIRP

> all system and safety risk controls for the interface have been identified

> all relevant stakeholders have been appropriately consulted

> safety requirements can be traced to relevant safety V&V activities

> all test results, faults and corrective actions generated from safety V&V and system integration activity have been captured

> all faults and corrective actions have been rectified, prior to the project and its complex systems being commissioned into service

> any conditions imposed on the use of railway assets by the safety V&V and system integration activity have been implemented, prior to the project and its complex systems being commissioned into service.

If the systems to be integrated involve multiple RTOs, each RTO must assess and understand the safety risks to its individual railway operations.

In addition, as each RTO is required to have effective management and control of its respective railway operations, the risk controls associated with system interface and integration may be apportioned to different RTOs with each owning specific aspects of the controls.

In such a situation, RTOs must seek to enter into a safety interface agreement with other relevant RTOs which will document how the interface risks will be collectively managed SFAIRP.