Application of Systems Engineering to Railway Projects

R N DUMOLO

Mott MacDonald, Croydon, United Kingdom

(Received from the Guest Editor on July 31, 2006)

Abstract: Complexity of new and modified railway systems increases with the application of modern systems technology. Such complexity must be assessed with respect to performance, safety and risk to assure achievement of stakeholder goals and the safety of the traveling public. The formal and rigorous application of 'systems engineering' techniques to modern rail projects provides a framework to eliminate some of the problems that have emerged in some of the more recent rail projects worldwide. These problems have led to delays in bringing projects into commercial revenue service. Systems engineering provides a framework within which a total rail system can be developed to progressively assure an acceptably safe and, as far as is practicable, a low risk rail system that additionally achieves the specified performance criteria. This paper discusses some of the basic elements that should be applied within an overall systems engineering framework to add confidence in delivering a project not only to achieve the goals of the stakeholders and the customers, but also to assure high safety and minimal risk. It explores some of the areas in past projects that could have potentially benefited from the earlier application these formal techniques.

Key Words: Systems Engineering, Performance, Safety, Risk Management

1. Introduction

Modern railway systems are becoming increasingly complex as current technologies, particularly in control and communications, are applied to all railway systems. These modern developments have enabled the integration of systems to improve functionality and efficiency of the rail system as a whole. Stakeholders are becoming more demanding and defining stringent system performance requirements to support the business cases for a project. Factors such as headways are being reduced, average and top speeds increased, and acceleration raised, to increase capacity. Under these circumstances, needless to say, safety margins can be eroded. Such complexity must be assessed with respect to safety and risk to assure the protection of the travelling public. The development of performance models and safety and risk assessments for the total rail system become more challenging with complexity and this can be made even more onerous with some contracting strategies that can be applied for procurement of a total rail system.

This paper discusses some of the basic elements that should be applied within an overall systems engineering framework, to achieve the goals of the stakeholders and the customers and add to the confidence in delivering successful projects.

* Communicating author's email: dick.dumolo@mottmac.com
Modern rail transport systems, mainline railways and urban metros and light rail schemes are generally fundamental to Governments’ policy to encourage the traveling public to use public transport as opposed to the private car. Under these circumstances it is critical to develop rail transport systems that have high performance criteria, not only in terms of journey time but also, more importantly, in terms of availability. Defining and managing these requirements is best addressed within a systems engineering environment.

Safety is of prime importance in all railway systems and the efficient delivery of the safety studies to support an operating certificate can be enhanced with the rigorous application of systems engineering to rail projects. This paper explores some of the areas related to the development of safety studies in past projects that could have potentially benefited from the earlier application of the formal techniques of systems engineering.

2. Systems Engineering

As modern rail systems become more complex there is a need to be able to manage all of the facets of a ‘system’ to enable the Stakeholder Requirements to be achieved at all stages of a project life-cycle, but in particular at the successful culmination of a project during the operational stage. The facets of a ‘system’ include hardware, software, firmware, people, information, techniques, facilities, services and all other support elements. The interaction of these facets must be addressed in a manner that assures completeness and this can best be achieved using formal methods that nowadays form the basis of ‘systems engineering’. Systems engineering encompasses a set of processes that are applied during the system life-cycle. These processes are aimed at understanding system requirements to enable the development of the system as an integrated whole, as distinct from a loose collection of parts, that achieves the defined requirements. Safety is clearly of prime importance to transport systems involving the carriage of people and this is one element of the systems engineering process that is enhanced through the application of formal systems engineering methods.

The formal application of ‘systems engineering’ techniques should be applied more rigorously to modern rail projects, both main line and urban metros, to eliminate a number of the problems, particularly related to safety, that have emerged in some of the more recent rail projects worldwide. These problems have led to delays in bringing projects into commercial revenue service. Systems engineering provides a framework within which a total rail system can be developed to meet not only the stakeholder requirements but also address the fundamental processes needed to assure the development of an acceptably safe and, as far as is practicable, risk free rail system. In addition to the development of new systems these ‘systems engineering’ techniques should be applied to rail systems undergoing major change, since the issues involved in the integration of old and new can be complex.

Requirements management, a key process in systems engineering, provides a powerful process that, when applied during the life-cycle of a project, will give not only the Stakeholders but also the design and construction contractors’ confidence in the delivery of a successful system. Requirements should address all aspects of a system including safety, and performance factors such as reliability, availability, maintainability, etc… Other elements of systems engineering such as interface and configuration management all contribute to the development of robust safety assessments. The systems engineering process enables the progressive assessment of safety at each of the main
stages of the project and enables safety issues to be identified and solved as early as possible and at a time when solutions can be cost effective.

Systems assurance is an important part of systems engineering in developing a safety case. A project needs to ensure that appropriate evidence of safety is obtained progressively as the project develops. Such evidence needs to be readily traceable so that it can be referenced in the safety case. In the past safety cases have been difficult to compile because evidence produced early on in a project can often go ‘missing’ and it is then time consuming to redevelop such evidence. It is therefore important to have robust assurance processes in place from the early stages of a project.

3. Systems Engineering Life-Cycle

Systems engineering is only effective if it is applied rigorously during all lifecycle phases of a project – from its inception, through to operation and change. The systems engineering framework provides a sound basis for the application of safety and risk assessments at appropriate stages during the project life-cycle. In the past, in some projects, safety assessments have not been applied in a consistent and progressive manner and as a consequence safety opportunities have been missed. The term ‘safety opportunities’ does not imply an unsafe system, but the solution to safety issues may not have been optimal because systems have been implemented leaving only procedural solutions to safety management issues that arise late in the project. For instance, projects that have started with a good approach to safety but then reduce the input because no immediate benefits are seen, lose out later when it is recognized that there are safety issues to resolve. At this late stage the models or evidence needed to develop sound safety arguments to support design or implementation change proposals do not exist. Time is then lost while extensive work is under-taken to develop these models to an appropriate level of detail to generate the safety arguments needed for decision making.

Other cases of inappropriate safety management practice have occurred when a project does not start the safety work at all until they are forced to later in the project – often because it is realized that it is an integral part of the process to gain an operating licence. Under these circumstances the emerging safety studies can identify hazards that by this time can only be managed through procedures where, given an earlier opportunity, the hazard could have been designed out.

Safety and risk are important elements within a systems engineering approach. Rail systems must be developed with high safety levels and consequent low safety risk to the users. The early development of safety studies are used to ensure that the base-lined design of the integrated system achieves safety risk levels that are ‘as low as reasonably practicable’ (ALARP). Additionally these safety studies can assist in the assurance of change, to designs and operational strategies, which inevitably occur during the implementation of major projects. The safety process must therefore follow, and be integral to, the systems engineering process at all life-cycle stages.

4. Impact of Operations

The development of a robust operations strategy is necessary to ensure that railway systems are designed to achieve the required performance requirements. The failure to define the operations requirements at the start of a project could lead to a failure to achieve stakeholder requirements and this in turn could impact on the financial viability of the project. Once the operations strategy is fixed this will define some of the parameters
required for systems modeling – for example timetable modeling, traction power simulation, station passenger flow analysis. The outputs from these studies will impact on the requirements for the development of the stations and railway systems.

The safe operation of a system relies on the development of a comprehensive operations strategy at an early stage in a project. These operations strategies often involve assumptions that will be realized and confirmed as the systems designs are developed from an interpretation of the project requirements. The successful delivery of a project with sound operations processes, that are also safe, requires a consistent input from an operations specialist. Projects are normally good at getting the initial strategies developed but often fail to provide the consistent operator input during the mid-stages of the project life-cycle. Operations input then increases as the project nears completion. The system engineering and systems integration approach, when applied to a project, will help in maintaining an appropriate level of operations input throughout the project life-cycle. This makes a major contribution to the development of designs that are operator friendly, leading to higher levels of safety.

5. Impact of Human Factors on Safety

The ‘human factor’ is an increasingly important element in systems engineering as projects become more complex. The potential for human interaction in all phases of a project does not diminish with complexity – it always seems to increase. At an early stage in the design of a project, important decisions are made with respect to the tasks that the operators and maintainers will be expected to undertake during operation. A significant number of these tasks will be safety critical or safety related and it is essential that these tasks are identified early and included in the safety assessments.

The role of automation versus human control is always a challenging issue. Safety must be addressed in these instances. One important aspect is the undertaking of an early task analysis of all operators and maintainers. This activity is to ensure that no staff member is overloaded to the extent that errors frequently occur in the workplace that could cause accidents. The application of a systems engineering approach should capture these operator and maintainer requirements early in the project. Once captured, these requirements should be assessed within the overall systems engineering framework to ensure the project output performance will be achieved.

6. Impact of Procurement Strategy on Safety

Railway systems comprise two principal areas of engineering, namely civil/structural and electrical / mechanical engineering and often these are procured separately. For the rail systems, there are typically two principal procurement strategies for the E&M elements that are often considered in rail projects - firstly the scenario where the total E&M package is awarded to a single supplier and secondly where specific E&M systems are awarded to separate suppliers. Clearly the systems engineering / integration strategies for each of these scenarios differ in a significant manner. In both cases there will be the need for a project systems engineer / integrator, but the role will vary significantly for both options. This critical role is that of undertaking the systems engineering / integration at the top railway system level, and additionally monitoring the progress of the systems engineering / integration tasks being undertaken by others. This applies particularly for the E&M systems and is necessary to give confidence that no major issues will prevent successful system operation on the planned schedule date for fully integrated operation.
All members of the project team (client, contractors and sub-contractors) will need to have within their technical teams a function of Systems Engineer/Integrator to undertake all systems engineering and integration activities related to their scope of supply. The basic systems engineering and integration activities that need to be undertaken by all suppliers at a level of detail appropriate to their scope of supply are typically as follows:

- Requirements Management
- Interface Management
- Performance Management
- RAM Management
- System Safety Management
- Software Management
- Human Factors Engineering
- EMC Management
- Configuration Control
- Integrated Systems Testing

Each of these activities will need to be managed from the point of view that either the activities will be undertaken directly by the contractor or subcontracted to their suppliers. In the latter case the client will not only monitor the suppliers’ activities but also have the major task developing appropriate ‘system-level’ assessments for their integrated systems. It must be recognised that all systems engineering activities cascade down the chain of supply.

The following sections provide a preliminary indication of how this cascade effect of systems engineering/systems integration activities impact on the role of the Systems Integrator for the E&M contracting strategies.

### 6.1 Procurement Strategy - Scenario 1

For this scenario, in addition to the civil contracts, a single contract is awarded to an E&M supplier to procure, design, manufacture, implement, test and commission all of the railway systems. The Project System Integrator appointed by the client will undertake the role as indicated in the diagram.
The role of Project Systems Integrator for the various interfaces is as follows:

6.1.1 Total System Level

At this level the role of the Project Systems Integrator is to ensure that the total rail system, as defined in the contracted scope of work, functions as an integrated system and meets the defined requirements. The activities to be conducted at this level include:

- Requirements Management, Verification and Validation
  - Identify contractual system level requirements and develop sub-requirements to civil and E&M levels
  - Ensure that all suppliers acknowledge their responsibilities concerning achievement of the requirements related to their systems
  - Undertake audits on E&M supplier systems integration team

- Interface Management
  - Manage the identified interfaces in all areas of the project and ensure that these are being managed by one agreed responsible party
  - In particular identify requirements to be allocated between civil and E&M contractors

- Performance Management
  - Ensure the E&M supplier undertakes performance studies to theoretically determine performance achievement.

- RAM Management
  - Undertake top level RAM studies in order to allocate RAM targets between civil and E&M contractor
  - Audit E&M contractor to ensure RAM targets can be achieved theoretically

- System Safety Management
  - Undertake top level system safety assessments using inputs from all contractors
  - Develop the top level system safety case

- Software Management
  - Determine the requirements for safety critical software
  - Audit the E&M contractors software development processes

- Human Factors Engineering
  - From safety studies determine areas where human factors issues are safety critical
  - Audit E&M Contractor to ensure appropriate human factor studies are being implemented

- EMC Management
  - Develop an EMC Management Plan
  - Audit the E&M contractor to ensure EMC management processes are in place

- Configuration Management
  - Implement a configuration management system and ensure that all contractors submissions are included
  - Audit E&M contractor to ensure configuration management processes are being applied in all areas of the team
  - Audit change control processes

- Integrated Systems Testing
  - Develop the total system integrated testing plan
  - Audit E&M contractors integrated testing plans and ensure that all interfaces between civil and E&M scopes of work are identified and being managed
6.1.2 Civil Contractors and E&M Contractor

The civil contractors undertake all systems engineering / systems integration activities for civil scope of supply and in particular those E&M elements that are normally included in the civil contractors’ scope of supply such as:

- Lifts and escalators
- Station power supplies
- Station lighting systems
- Fire detection and suppression system
- Tunnel Ventilation,
- etc.

The E&M contractor will undertake all systems engineering and integration activities for the railway systems within his scope of supply. The project risk in this area is high and under this contracting arrangement the E&M supplier will be responsible for managing this risk.

The systems engineering and integration activities to be undertaken are as follows:

- Requirements Management, Verification and Validation
  - Develop requirements for all systems from contract documents and ensure these form part of the procurement contract
  - Develop a process to verify achievement of all requirements during the design development phase
- Interface Management
  - Manage the identification of all interfaces between civil E&M systems and civil E&M / railway E&M systems and assign responsibility for management and resolution
- Performance Management
  - Undertake any performance related studies to ensure system will meet performance requirements
- RAM Management
  - Set up RAM Management system and develop RAM Plan
  - Undertake RAM studies for all E&M systems
- System Safety Management
  - Set up safety management system for E&M systems and develop Safety Plan
  - Develop all safety assessments for E&M systems
- Software Management
  - Set up Software Management Plan for E&M System
  - Identify any safety critical or safety related systems software and allocate appropriate software Safety Integrity Level (SIL)
- Human Factors Engineering
  - Identify areas where human factors issue may impact on safety and operability (e.g. operator controls, maintenance, etc.)
  - Undertake appropriate HF studies to influence design approaches
- EMC Management
  - Set up EMC Management Plan
  - Undertake appropriate EMC studies during design phase
- Configuration Management
  - Set up a Configuration Management system
  - Implement configuration management system
6.1.3 Civil and E&M Contractor Interfaces

The key role of the Project Systems Integrator will be to monitor and audit the systems engineering and integration activities being undertaken by the civil and E&M contractors. Monitoring would be achieved through regular progress meetings and the receipt of all key deliverables for review and comment. In-depth audits would need to be conducted at intervals to ensure the robust application of the systems engineering and safety processes by the contractors during all of the projects phases.

6.2 Procurement Strategy - Scenario 2

This contracting scenario differs from Scenario 1 in that it involves the project contracting multiple suppliers for the railway E&M systems. A fundamental consequence of this contracting strategy is that it opens up many more interfaces to be actively managed by the Project Systems Integrator. The minimisation of project risk, and in particular safety risk, will involve the formation of a strong Systems Integration Team within the Project management organisation.

Fig. 2: Interfaces for Procurement Strategy – Scenario 2

The roles of the Project Systems Integrator, related to the key interfaces represented on the above diagram, are as follows:

6.2.1 Total Systems Level

The total systems level systems engineering and integration activities are the same as for Contracting Strategy - Scenario 1 for the civil and E&M interface. However there will be an additional area of work as described below related to the integration of the rail systems.

6.2.2 Civil Contractors

This activity will be the same as for Contracting Strategy - Scenario 1.
6.2.3 E&M Contractors

Each E&M contractor will be responsible for undertaking systems engineering and systems integration activities for their own scope of supply. The contracts for the E&M suppliers must not only define this role, but also commit them to identifying any interfaces with other parties in the contract that are necessary for them to achieve their systems requirements in terms of performance and RAM. These aspects must be further reinforced by committing all suppliers to co-operate with the Project Systems Integrator to achieve a fully integrated transport system. Support in this area will involve the suppliers sending representatives to regular systems integration progress meetings chaired by the Project Systems Integrator.

6.2.4 Civil and Railway Systems E&M Interfaces

The management of the interfaces between the railway systems suppliers represents a major task for this contracting scenario. There will be particular tasks that the Project Systems Integrator will need to undertake in order to ensure that the system will deliver the contractual performance requirements. Some of these tasks are as follows:

- Top Level Requirements Engineering and development to Railway Systems Requirements
- Railway System Performance Modelling
- Rolling Stock Performance
- Traction Power Performance
- Signalling System Performance
- Communications Systems Performance
- Integrated Transport System Safety Studies
- Integrated Transport System RAM studies
- EMC Management
- System Operation and Maintenance Plans
- System Degraded Performance Analysis and Restoration Plans
- Fire Engineering Strategies and Plans
- Development of Emergency Evacuation Plans
- Development of Systems Integrated Testing
- System Safety Case and
- Development of System Acceptance Plans.

The above tasks represent the key top level systems engineering and integration activities related to the railway E&M systems that will need to be progressed by the Project Systems Integrator. These tasks will be undertaken by specialists, in many cases, using specialist tools and computational methods. The technical capability of the Project Systems Integrator will need to be strengthened with specialist engineers with expertise in rolling stock, signalling, traction power and communications.

The level of effort required for the Project Systems Integrator increases significantly for this scenario. The development of robust contractual conditions for each supplier to deliver systems engineering and systems integration activities and to support the Project Systems Integrator in all these areas of work will be critical. Success in this area could ease the level of effort required by the Project Systems Integrator. Good systems engineering and systems integration deliverables from the suppliers will reduce the effort required to develop the top level systems deliverables.
7. **Observations from Past Railway Projects**

Past project experience in the rail sector should be used to enhance the management of systems engineering and safety in an efficient manner to enable delivery of acceptable levels of performance and safety that meet the project requirements. This added efficiency should also lead to cost effective solutions to safety issues whilst assuring the achievement of the overall project performance requirements. Some observations of poor project performance related to safety management are identified below:

- Safety and risk studies have started too late for those projects undertaken without a robust systems engineering framework. System designs have been specified without capturing all of the system requirements and this has led to the late consideration of potential safety issues.
- Large long term projects have started with good intentions and early safety studies have been undertaken. This ideal approach to safety management and assessment has then been reduced in scope as there were few perceived benefits from continuing the detailed studies. The essential safety studies were not developed in detail with the consequence that later there were no appropriate safety models to assess safety issues related to late changes in the projects.
- Big projects have had dispersed safety teams that were unable to ‘see the big picture’. This has led to a ‘silod’ approach to safety and failure to adequately address the impact of safety issues across the multiple interfaces that are common in railway systems. This has led to difficulty in compiling the top level safety arguments that are needed to be included in the Safety Case against which the Operating Certificate is often granted.
- The lack of continuous involvement of operators can lead to the development of systems that have not been optimised with respect to the operational and maintenance regimes. This can impact on the management of safety.
- The late development of requirements restricts novel thinking in safety critical areas. The early development of safety requirements enables options to be developed and analysed to develop solutions that meet the safety requirements, and are not ‘over-engineered’ at excessive cost.

8. **Conclusion**

Performance and safety in rail projects in the past has been achieved, though in some instances the approach adopted has not been efficient. The growing application of systems engineering to new projects provides a valuable opportunity to ensure a more robust approach to performance, safety and risk management. However, this does depend on projects applying systems engineering for the total project life-cycle.

**Mr. R N Dumolo** is a Divisional Director of the Railways Division of Mott MacDonald and is responsible for Safety and Systems Engineering. His career started in the nuclear sector where he undertook safety studies on Magnox and AGR gas cooled reactors. He also undertook safety studies on both pressurized and boiling water reactors in the UK and Europe. Later in his career he applied the well developed nuclear safety assessment techniques to rail systems in the UK, initially on the Channel Tunnel Rail project. The formalization of the application of safety assessment in the UK rail sector occurred when the Railway Safety Case Legislation that was introduced in the UK following a number of severe rail accidents.