Linking Risk Analysis to Safety Management

Vladimir Trbojevic
Risk Support Limited
London, UK

Abstract

Linking risk analysis to safety management using bow ties leads to the safety management system that can better focus on the demonstration that risks are as low as reasonably practicable and that sufficient safety has been incorporated in the design and operation of the facility.

1 Introduction

The UK safety case regime requires duty holders to demonstrate that their management system will ensure compliance with the relevant statutory provisions and that all hazards with the potential to cause major accidents have been identified, the risks evaluated and measures taken to reduce risks to persons affected by those hazards to the lowest level that is reasonably practicable. This means that a duty holder has to show through reasoned and supported arguments that there is nothing else that could reasonably be done to reduce risks further. This process has brought about significant improvement in safety but certain issues and areas for improvement have been identified, for example:

1. Amount of information transfer from hazard identification and risk analysis through to the safety management system is insufficient. Risk analysis is poorly understood by the workforce and is not being used in day to day business.
2. Safety management system should primarily be for the duty holder to assure itself that its operations are safe, and demonstrating this to the Regulator is only secondary matter.
3. Safety Case acceptance seems to be the key objective, and continuous improvement in health and safety is becoming a secondary issue.
4. A number of human factors techniques which are known to be effective such as workforce involvement, behavioural safety programmes, safety leadership, and human factors inclusion in task risk assessments are mostly absent from the demonstration of safety.
5. No evidence could be found in the safety management system of higher-level human factors considerations, for example end-user or human factors practitioner involvement in procurement and design. No evidence could be found of embedding human factors into organisational process, for example, structured in-service feedback for development of usability, reliability and safety.

6. Safety management systems can become paper exercises and sterile documentation full of procedures, which can lead to a) complacency, b) erosion of good practice due to time-consuming procedures of paper work, c) misplaced confidence due to absence of accidents, etc.
7. The demonstration of reasonable practicability in many cases seems to be lost in numerical estimates of risk and is considered as an add-on to the numerical process instead of being applied from the description of the facility, good practice, through to hazard identification and demonstration of sufficient safety barriers, etc.

Therefore there is a need to remedy the above shortcomings and to streamline and energise the safety management system and to integrate it with the safety demonstration. This paper focuses on linking risk analysis and the safety management system to ensure by suitable and sufficient evidence that risk is as low as reasonably practicable.

2 The Approach

2.1 Safety Objectives and Process Model

The fist step in this approach is the definition of safety objectives and the facility specific processes and related activities and personnel task required for the processes to run. Safety objectives influence the activities and tasks by facilitating explicit focusing on safety. Management accountability and personnel responsibilities are distributed, and the duty of a responsible person is to carry out the task/activity in a specified manner and record any deviations. The development of the activity/task (process) model is iterative and in many cases the safety related tasks are driven by the risk model.

2.2 Hazard Identification

It is assumed that hazard identification has come up with the list of threats (hazard triggers) and that the hazards are mapped into initiating events. Taking an example from the railway industry, the top event is “passenger train derailment” and the threats (hazard triggers) are “ track faults”, “rolling stock faults”, “obstructions on tracks”, etc. The possible consequences of this event could be “injuries and fatalities”, “damage to trains and tracks”, etc. The corresponding cause-consequence diagram also called a “bow tie” [1] is presented in Figure 1. It depicts the results of hazard identification but instead of failures it focuses on lines of defence (barriers). The main objective of hazard identification is to identify all possible lines of defence that are and could be put in place to demonstrate sufficient safety.

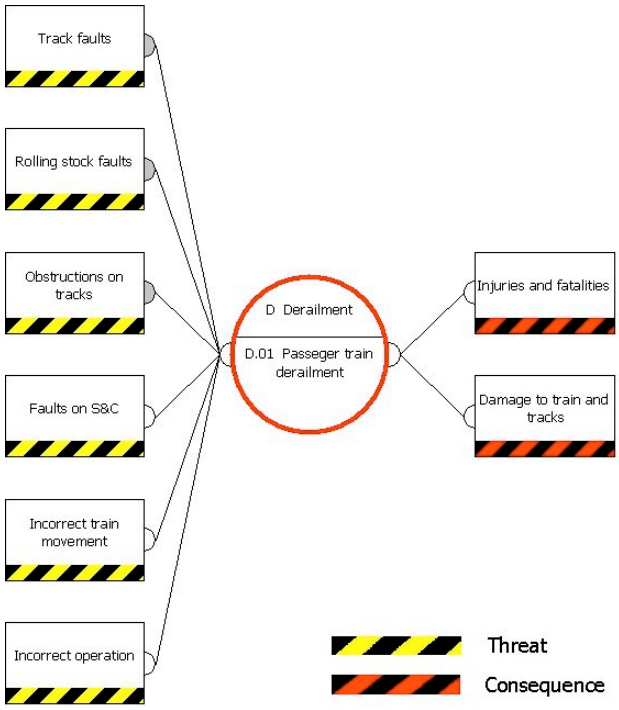

Figure 1. Threats, initiating event and consequences

To prevent threats form being realised and escalating to the top event, barriers are provided (denoted by a box with a thick black bar on the right), Figure 2. The barriers against "track faults" are to "ensure quality of tracks" and "regular track maintenance". However, the barrier "ensure quality of tracks" may be eroded because of, for example, the "broken rail", "spread gauge", "buckled track", etc. These failure modes are called escalation factors and represented by a box with the thick red line at the bottom. An escalation factor is a situation or condition of increased risk. If the barrier failure mode is identified than in most cases, in order to demonstrate safety, it is required to provide a secondary barrier or escalation factor control to prevent the failure mode. In the example in Figure 2 for the barrier failure mode "track buckled", the secondary barriers are "sufficient number of expansion switches", "maintain good ballast condition", etc. The barriers may have the different coloured bars on the right hand side to represent different groups of workers, subcontractors, or different types of barriers. If all barriers are breached, and the initiating event (loss of control) is reached, then recovery measures (barriers) should be provided to mitigate unwanted consequences. Recovery measures may have failure modes and are treated in the similar way as the barriers on the left-hand side of the bow tie.

Explicit focusing on barriers and recovery measures facilitates a systematic evaluation of lines of defence which may be classified as follows:

- Engineered defences (hardware barriers, either passive e.g. good design practice, or active, e.g. preventative, mitigation, recovery systems, etc.).
- Systemic or procedural defence (software barriers).
- Human defences (liveware barriers).

A good safety solution should have a reasonable mix of defences with the engineered barriers as the front line of defence, and systemic and human barriers operating on the different level, for example, installation and maintenance of engineered barrier, supervision, etc. Systemic defences can fail if there is a lack of procedures leading to erosion of engineered defences. This approach focuses on all lines of defence and represents a natural way for inclusion of human and organisational factors.

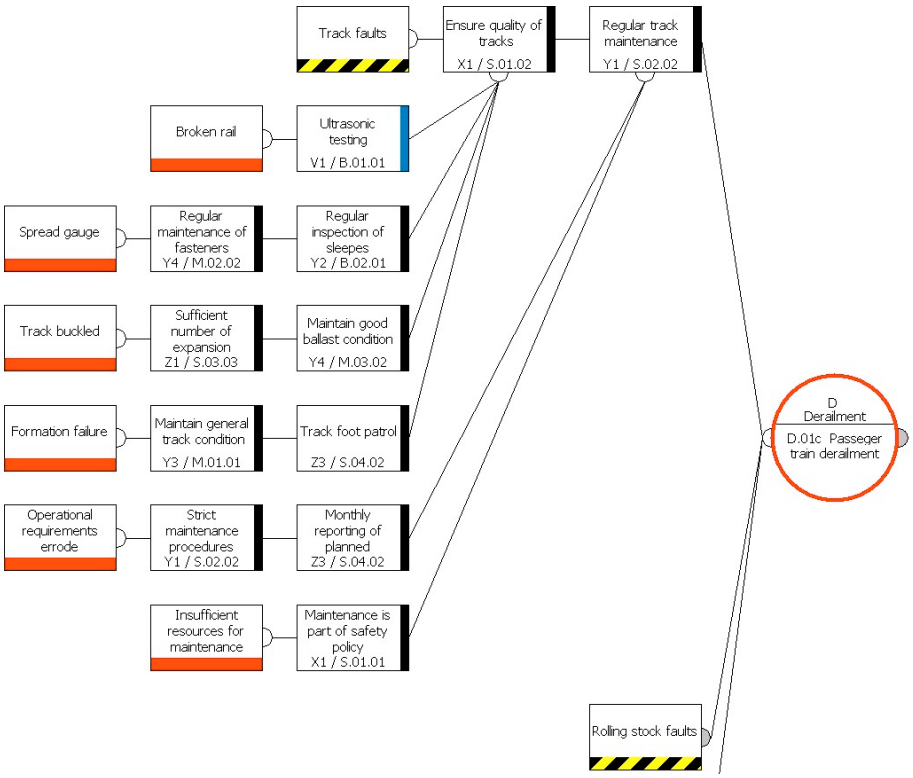

Figure 2. Barriers and escalation factor controls

2.3 Energising Lines of Defence

Having the risk model and the list of day-to-day activities and tasks, organisation for safety can be carried out. This means that a set of safety critical activities and tasks is identified, the purpose of which is to ensure that barriers are operational at all times. These tasks are then linked to the corresponding barriers, [2]. This process is

iterative and may require some "matching" before a proper link between the task and the barrier is established. In Figure 2, in the lower part of the barrier box, the post indicator of the responsible person (or contractor's organisation) and the corresponding tasks shown (e.g. X1, X2, Y1, etc denotes personnel group and position, and "S.01.02" denoted task 2 of activity S.01). As mentioned before the development of bow tie risk model and the corresponding process model proceeds in an iterative manner.

The activities and tasks taken to ensure that risk controls are effective at all times are called "safety-critical". An activity comprises a set of tasks with the same management objective.

2.4 Completing Operational Management System

The operational part of the safety management system (SMS) can now be developed as a natural extension of the above approach. In fact, each activity with its set of tasks represents a "procedure", except that each task is "hard wired" to the corresponding risk barrier. Therefore to complete the operational part of the management system, the following components, shown in Figure 3, are added.

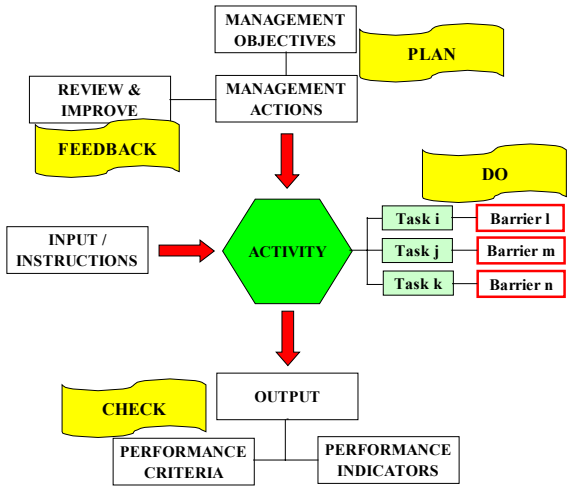

Figure 3. Safety critical activity

These components are as follows:

- Management objective for the activity and action required to implement it,
- Performance indicators and criteria for measuring the execution of tasks,
- Feedback loop for the improvement and operational changes,
- Input and output for the activity; for example, if the absence of a written procedure could result in infringement of the safety policy or breaches of legislative requirements or performance criteria, then the additional procedure

represents an input for the activity. Similarly, output from an activity may represent the input for another activity, etc.

In associating tasks with risk controls, distributing responsibilities, defining objectives and the sources and means of measurement, the integrity of the management system is demonstrated.

2.5 Analysing Safety Management Organisation

The final step is to analyse the hazard related to organisation and management of the facility and repeat safety demonstration process as executed for operational/process hazards. This step explicitly links the top management activities and responsibilities to the safety management system and focuses on identification of defences against management and organisational failures.

3 Conclusions

The following conclusion can be drawn from this approach:

- It constitutes a template for comprehensive demonstration of safety and inclusion of human, management and organisational factors in the SMS.
- It facilitates a full involvement and understanding of risk analysis by all stakeholders (management, workforce, contractors, etc.) - this will avoid complacency.
- It raises the awareness of the workforce to safety issues, i.e. every person will know where and how he/she fits in the hazard management process - this will energise the system.
- Accountability and responsibility will be visible and well defined – this facilitates taking responsibility.
- It facilitates day-to-day usage of the safety management system since task can be recorded and risk management decision taken on the daily basis.
- Better understanding of the hazards and the corresponding barriers reduces human errors during operations or maintenance.

References

1. Trbojevic, V.M., Linking Risk Assessment of Marine Operations to Safety Management in Ports, 6th Biennial Marine Transportation System Research and Technology Coordination Conference, Washington DC, 14-16 November 2001.
2. Trbojevic, V.M., New Approach to Risk Analysis and Safety Management in Ports, KONBiN'03, The 3rd Safety and Reliability International Conference, Gdynia, Poland, 27-30 May, 2003.