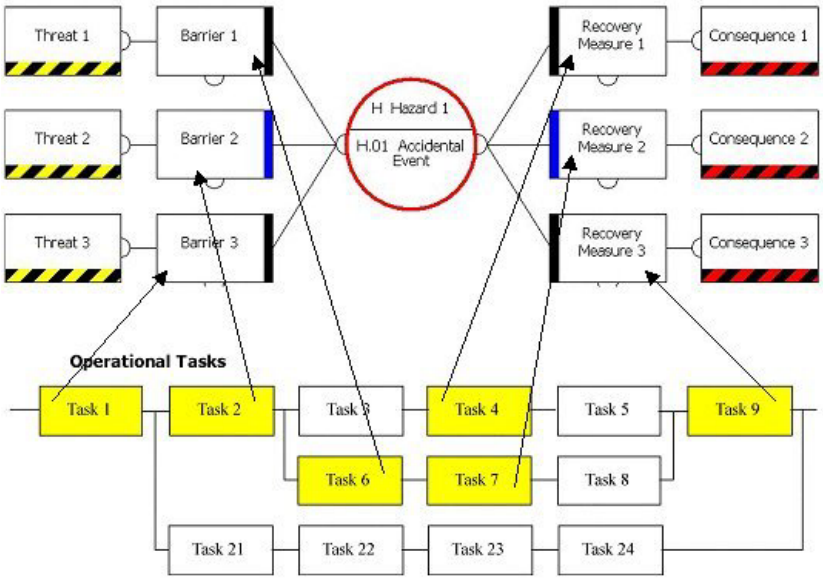
MANUAL



Active Bow Tie

A tool for displaying and improving hazard analysis and energising safety management

Risk *Support*

Risk Management Consultants

88 Kingwood Road
London SW6 6SS
United Kingdom
Telephone +44 (0)20 7385 1432
Facsimile +44 (0)20 7385 7844
Email vmt@risk-support.co.uk
http://www.risk-support.co.uk

MANUAL

Active Bow Tie

A tool for displaying and improving hazard analysis and energising safety management

July 2007

Version 1.7

Revision	Date	Approved
1.1	February 2004	V.M. Trbojevic
1.5	June 2004	V.M. Trbojevic
1.7	July 2007	V.M. Trbojevic

CONTENTS

1 INTRODUCTION 1

1.1 BACKGROUND 1
1.2 DESCRIPTION OF BOW TIE ANALYSIS 2
1.2.1 Hazard Analysis 2
1.2.2 Process Model 4
1.2.3 Linking Risk and Process Models 4
1.3 INTEGRATED SAFETY MANAGEMENT SYSTEM 4
1.3.1 Risk Evaluation 5
1.4 DATABASE STRUCTURE 6

2 STARTING 8

2.1 INSTALLING ACTIVE BOW TIE 8
2.2 USER MANUAL 9
2.3 SETTING UP A NEW CASE/DATA FILE 10
2.4 DEFINING REFERENCE DATA 11
2.4.1 Personnel 11
2.4.2 Competencies 12
2.4.3 Effectiveness 12
2.4.4 Activity Categories 13
2.4.5 Frequencies 13
2.4.6 Control Types 13
2.4.7 Risk Matrix 14

3 HAZARD ANALYSIS 17

3.1 HAZARD CATEGORIES AND TOP EVENTS 17
3.2 THREATS AND CONSEQUENCES 18
3.3 BARRIERS AND BARRIER DECAY MODES 19
3.4 RISK ANALYSIS 21

4 ACTIVITIES AND TASKS 23

4.1 ACTIVITIES 23
4.2 TASKS 24
4.3 ADDITIONAL ACTIVITY INPUT 25
4.3.1 Objectives 26
4.3.2 Management Actions 26
4.3.3 Inputs 26
4.3.4 Outputs 26
4.3.5 Performance 26
4.3.6 Deficiencies 27

5 LINKING TASKS AND CONTROLS 28

6 REPORTS 31

6.1 DISPLAYING INFORMATION IN BOW TIES 31
6.1.1 Box Style 31
6.1.2 PEAR 31
6.1.3 Barrier Effectiveness 31
6.1.4 Barrier Post Indicator 31
6.2 REPORTS 32

7 PRINTING BOW TIES, COPYING, PASTING, DELETING, ETC. 37

7.1 BOW TIES 37
7.2 COPYING, PASTING AND DELETING 37
7.3 REORDERING 37

1 INTRODUCTION

1.1 Background

Bow tie approach[1] was originally devised to energise the safety management system. The theory behind the bow tie approach can be found in the "Swiss cheese model" of Reason[2]. The approach is mostly used in the hazard identification and the development of the hazard register, to link hazard barriers and operational systems and procedures in place to eliminate the hazard or reduce its frequency of occurrence, or mitigate its potential consequences. As such it also a hazard and risk control display tool. A more mature extension of the approach was based on a desire to overcome the following shortcomings in a safety case regime:

1. The transfer of information from hazard and risk analysis through to the workings of the management system (i.e. to operations) has been insufficient. This means that link between the major accident hazards and the safety management system (SMS) is not usually explicitly presented. The emergency response plans typically provide the chain of communication in an emergency, the organisational structure, tasks of responsible persons, and the list of actions to be carried out in the event of a specific emergency situation following a major hazard event. A link between the technical system descriptions in the Safety Report, and the demonstration of the working of the management system in the context of major hazard control, is usually missing. This is not unusual because the methodologies for hazard analysis and risk assessment, in general, do not deal with the complex technical and organisational systems in a unified manner.
2. The Quantitative Risk Assessment may take into account operator error in the causation part of the assessment, while it is rare to account for human factors in the escalation part of the assessment, unless a specific operator action is intended to be a safety barrier. However, even then, the quality of organisation and management is not accounted for. For example, to incorporate the "probability of partial malfunction of the emergency system" is unheard of. This does not mean that the quality of organisation, or "organisational factors" cannot be evaluated; they can be accounted for in the overall shifting of the risk profile or the scaling of the failure rates.
3. The operational process model may be established for the purpose of quality management system, but not for the purpose of major hazards and the SMS. There is, in general, a "fuzzy" link between the hazards and operational activities and tasks, and even "fuzzier" link between risk controls and operational tasks.

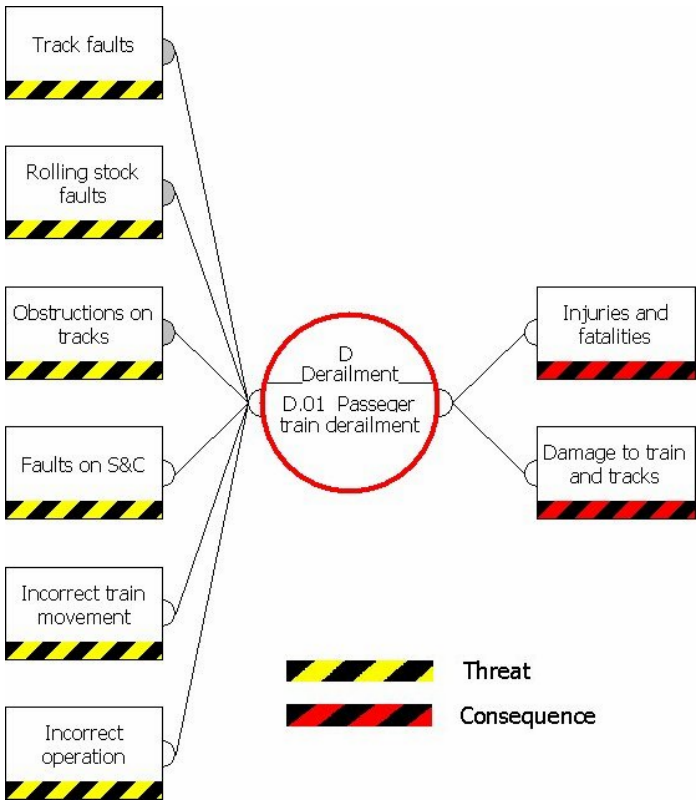
[1] Shell International Exploration and Production BV, Thesis HSE Manual, EP-95 0323, 1995.
[2] James Reason, Human Error, Cambridge University Press, 1990.

1.2 Description of Bow Tie Analysis

1.2.1 Hazard Analysis

In this example, *Figure 1.1*, hazard is derailment and hazard realisation is the top event "passenger train derailment". The threats (that can lead to the top event) are "obstruction on tracks", "rolling stock faults", "track faults", etc. The possible consequences of this event could be "injuries and fatalities", "damage to trains and tracks", etc.

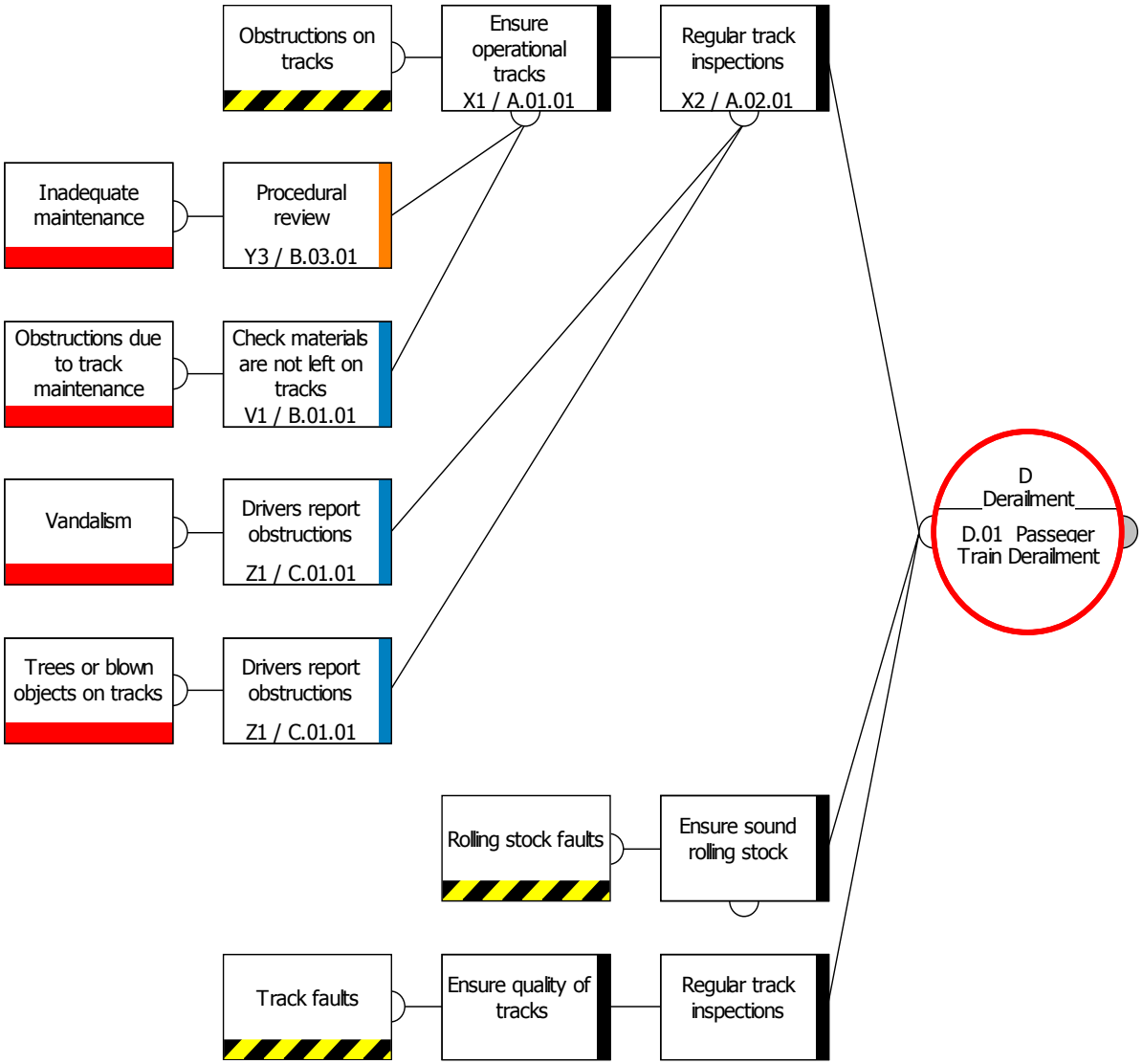
Figure 1.1 Derailment Bow tie



To protect from threats, barriers are provided (denoted by a box with a thick black bar on the right), *Figure 1.2*. The barriers against "obstructions on tracks" are to "ensure operational tracks" and "regular track inspections". However, the barrier "ensure operational tracks" may decay because of the "inadequate maintenance", or may fail due to "obstructions due to track maintenance". This barrier decay/failure mode[3] is denoted by the box with the thick red line at the bottom. If the barrier decay/failure mode is identified than it may be required to provide a secondary barrier to prevent the decay/failure mode. These secondary barriers reinforce primary barriers (which protect from threats). The numbers of the primary and secondary barriers are governed by the risk acceptance criteria.

[3] Barrier decay/failure mode is also called "Escalation factor" (e.g. in Thesis)

Figure 1.2 Barriers and Barrier Decay/Failure Modes



The barriers with different coloured bars on the right hand side are intended to represent different type of barriers, or groups of workers, subcontractors, etc.

Similarly, if all barriers are breached, and the top event (loss of control) is reached, then (protection / mitigation) barriers should be provided to protect from top event and/or mitigate unwanted consequences. These barriers and their decay/failure and are treated in the similar way as the barriers on the left-hand side of the bow tie.

1.2.2 Process Model

In parallel with the bow tie risk analysis, the "systems model" is developed which describes all processes of the Company. Furthermore a set of activities and tasks are identified required to keep the "process" functioning on a daily basis. For each activity and each task within an activity responsible persons is identified. 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 process model is iterative and in many cases the risk model drives the new tasks and vice versa.

1.2.3 Linking Risk and Process Models

In the next step the tasks are matched to the barriers. This means that for each barrier there should be a task the purpose of which is to ensure that the barrier is operational at all times. This process is also iterative and may require some "matching" before a proper link between the task and the barrier is established. In *Figure 1.2*, 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 "A.01.02" denoted task 2 of activity A.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.

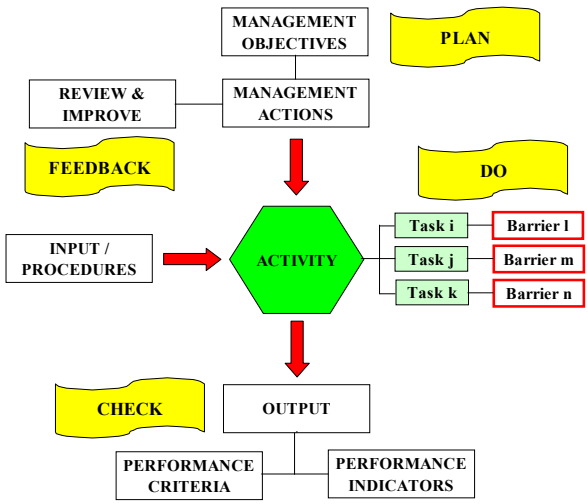
1.3 Integrated Safety Management System

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" in the old sense, except that each task is "hard wired" to the corresponding risk barrier. Therefore to close the continuous improvement loop, the following components of the SMS, shown in *Figure 1.3*, are added:

- 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.

Figure 1.3 Safety Critical Activity



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.

A similar approach can be utilised to extend the safety management system to cover the management and organisational aspects.

1.3.1 Risk Evaluation

Risk evaluation is carried out by assessing the likelihood and the severity of consequences using either risk matrix approach, or the results of quantitative risk analysis. Typically these risk can be low (acceptable), medium (tolerable if reduced to be As Low As Reasonably Practicable – ALARP) and high/intolerable (operation is not allowed). The evaluated risks are then assessed against risk acceptability criteria.

Risk criteria are developed in terms of the required number of barriers for each risk level. Risk criteria can also be formulated in conjunction with safety rating or the effectiveness of risk controls which depends on the barrier effectiveness, availability, independence, means of control over barrier, etc. An example of risk criteria without barrier rating is presented in *Figure 1.4*.

Risk reduction is then carried out in accordance with the risk tolerability doctrine, or the national safety legislation, etc.

Figure 1.4 An Example of Risk Criteria

Region		Criteria
ALARP	1	Requires a minimum of two rimary barriers in place for all threats
	2	Requires a minimum of one primary barrier (recovery measure) for identified consequence
	3	Requires a minimum of one effective control in place for all barrier decay/failure modes
Intolerable	1	Requires a minimum of three primary barriers in place for all threats
	2	Requires a minimum of two primary barriers (recovery measures) for each identified consequence
	3	Requires a minimum of one secondary barrier in place for all barrier decay/failure modes

1.4 Database Structure

The data structure in Active Bow Tie starts with the *Study* (or Safety Case) which covers one or several *Locations*. Each location is exposed to *Hazards* and has an *Activity Set*. A set of *Hazards* comprises of one or several *Hazard Groups*, each of which is mapped into one or several *Top Events*.

Each *Top Event* can be triggered by a set of *Threats* (within a *Threat Group*), and to prevent hazard realisation *Barriers* are put in place. Factors that can reduce barrier effectiveness called *Barrier Decay Modes* (B.D.M.). To protect the barriers from this decay modes the *Secondary Barriers* can be specified.

Escalation from *Top Event* can lead to a *Consequence Group* containing one or several unwanted *Consequences*. There are *Barriers* in place top protect from top event and mitigate the consequences. These barriers can be associated with the barrier decay modes, which are controlled by secondary barriers.

Each *Activity Set* contains one or several *Activity Groups* each of which comprise one or several *Activities*. Each *Activity* comprises of *Tasks*, some of which are safety critical; i.e. the purpose of those tasks is to ensure that barriers are operational at all times. An activity also comprises of the associated safety objectives, management actions, input, output, performance indicators and criteria

(*Figure 1.3*). A graphical representation of the data structure is presented in *Figure 1.5*.

Figure 1.5 Database Structure