A Framework for Risk Management in Railway Sector: Application to Road-Rail Level Crossings

A. Berrado, El Miloudi El Koursi, A. Cherkaoui, M. Khaddour

A Framework for Risk Management in Railway Sector: Application to Road-Rail Level Crossings

Abdelaziz Berrado*, EMI, Université Mohammed V, Rabat, Morocco, Assistant Professor, berrado@emi.ac.ma
El-Miloudi El-Koursi, INRETS, Lille, France, Research Director, miloudi@terre.inrets.fr
Abdelghani Cherkaoui, EMI, Université Mohammed V, Rabat, Morocco, Professor, cherkawi@emi.ac.ma
Moha Khaddour, ONCF, Rabat, Morocco, General Safety Inspector, khaddour@oncf.ma

Abstract

A major concern in rail industry worldwide is to ensure safety in railway operations in general and at road/rail level crossings in particular where the number of fatal accidents has been significantly increasing over the years. Accidents at level crossings are the result of complex interactions between factors arising from the design and operations of level crossings. An important first step towards eliminating the causes of these accidents is thru understanding and assessing the risks associated with a given level crossing and acting on them. This paper introduces a risk management framework that serves this purpose. The suggested framework involves several activities, including, hazard identification, risk analysis, evaluation, treatment and control. Having explained the suggested framework, this paper illustrates how it can be systematically applied to mitigate risk at a given Moroccan level crossing. The efficiency and success of the suggested risk management framework is pending its integration in a global rail safety management system also introduced in the paper.

1. Introduction

Railways are regarded as an economic, efficient, environmentally friendly and very safe mode of transport. However, in the recent past, the European Community has noted the loss of a substantial share of the railway market to other modes of transport. The liberalized rail transport market similar to those in the civil aviation and maritime sectors requires some major changes in current practices, such as introduction of more self-regulation for companies operating in the rail sector, and increased openness and transparency in all member state railways. A common safety policy is essential to the future of the industry in Europe. Harmonization of the regulatory framework is seen as a key part of creating this commonality. In recent years, the European Commission has begun to develop several railway initiatives, which are aimed at encouraging open market policy and harmonizing the railways in Europe to facilitate horizontal integration(i.e. interoperability of the networks facilitating smooth movement of passenger and freight trains), vertical separation(e.g. between management of infrastructure and train operation and outsourcing of maintenance and support functions) and a due and transparent certification process to improve safety approval and equipment acceptance. In addition to the major legislative changes that have been undertaken across the European community in the last few years, there are ongoing technological changes that are occurring. Therefore there is the potential for instability and confusion in the railway industry resulting in an overall increase in accident risk. These changes affect not only the organizational and technical innovations developed with the new systems, but also the new stakeholders and financial arrangements derived from the major changes.

Railway safety is even more questionable at road rail level crossing (LC) where the number of fatal accidents has been significant over the years. A major concern is to understand and remove the risks in railway operations in general and at LC in particular.

The subject of risk has increasingly become a point of shared interest between many entities representing different sectors. According to a definition of the United Nations, risk "refers to the expected losses from a particular hazard to a specified element at risk in a particular future time period. Losses may be estimated in terms of human lives, or infrastructure damaged or in financial terms". In this paper we introduce a risk management framework that can be used to build a generic risk model which will lead to increasing the understanding of risk profiles at railways and will allow for risk based decision making to take place via a structured representation of the causes and consequences of potential accidents arising from the operations of railways. We illustrate how the suggested framework can be used for risk assessment at road/rail level crossing. The suggested framework could be easily adjusted to model risk in other sectors as well. Furthermore, we explain how the suggested risk management framework can be integrated into a global safety management system in the railway sector.

The rest of this paper is organized in four sections. In the following section, we introduce the suggested risk management framework and explain its different components. In section 3, we focus on the integration of the suggested framework into the global safety management system in the railway sector. A Moroccan level crossing is then used in Section 4 to illustrate how the suggested risk management framework is applied to tackle risk at LC. A conclusion follows.

2. Risk and the Risk Management Process

The subject of risk has increasingly become a point of shared interest between many entities representing different sectors. This gave rise to different but converging definitions of risk [3, 4, 16, 17, 23]. Risk has been defined both qualitatively and quantitatively. Modares [16] defines risk qualitatively as the potential of loss or injury resulting from exposure to hazards. A hazard being considered as source of danger that is not associated to the likelihood with which that danger will actually lead to negative consequences. Quantitative definitions of risk associate hazards with their probability of nuisance to the people and the environment. For instance in [12], risk is defined to be a set of scenarios (S_i), each of which having a probability (or frequency P_i) and a consequence C_i. This quantitative definition to risk aims to estimate the degree or probability of loss related directly to the occurrence of hazards or potential failures of a system.

An organization faces essentially three different types of risk to its operations, namely internal risks, i.e. those associated with activities and locations for which the organization is solely responsible, external risks, i.e. those originating from systems, people or organizations and processes that are outside the organization's control and shared risks, i.e. risks associated with activities or locations for which there are shared responsibilities rather than sole ownership; to manage such risks the organizations have to ensure that compatible approaches are used.

The need for practical assistance in applying risk management in public and private sector organizations, has led to the development of standards on risk management such as The Risk Management Standard [10] and the Australian and New Zealand standard on risk management [1].

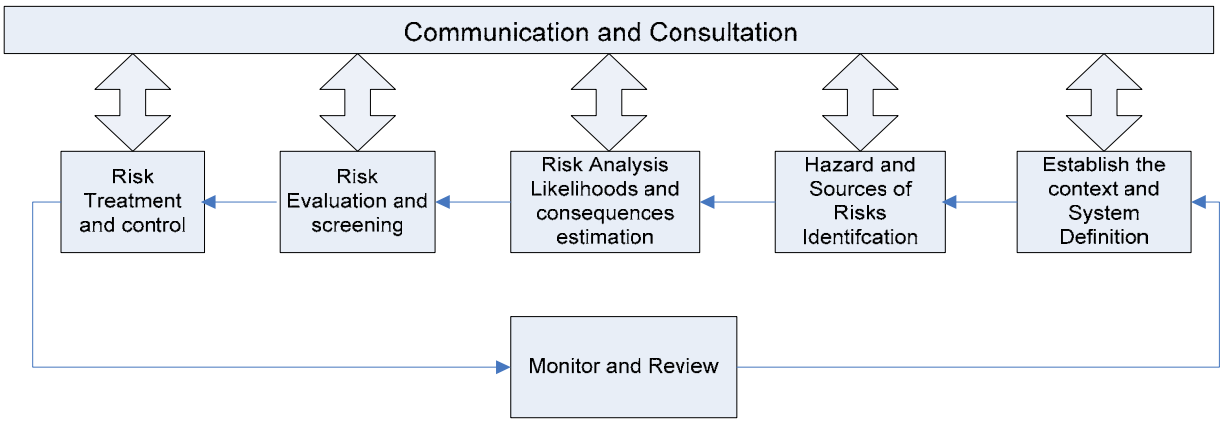

Figure 1. Flow Chart of a Generic Risk Management Process

The risk management process as set out in the standards consists mainly of five sequential stages, as illustrated in Figure 1, beginning with the establishment of the context within which risk has to be evaluated in order to set both the objectives and scope of the system; this entails an exhaustive and detailed description of the system that is at risk. Having delimited the system, one should identify the potential hazards or sources of risk; in this stage the list of initiating events, E_i, or scenarios of events leading to the undesired outcome is enumerated. Those events include essentially internal and/or external failures of both the technology used and the human force responsible for it. The next stage, usually referred to as risk analysis is reserved for estimating the likelihood, P_i, of the scenarios or events E_i, actually occurring and each scenario's consequence, C_i, is also estimated. The results of the risk analysis stage are thereafter used to

compare and rank the various risk drivers and compute the total expected risk value, R, defined as: $R = \sum R_i$ where $R_i = P_i \times C_i$ is the expected risk value associated with event E_i, the risk analysis is illustrated in Figure 1. In the evaluation stage minor risks may be screened out and more attention will be routed towards risks with highest expected risk value. Risk treatment is the final stage, where action plans are determined in response to the identified risks and mechanism to control those risks are put in place. It should be noted that this risk management process may well require regular monitoring and review especially when applied with dynamic systems which may evolve over time. Successful risk management requires that all parties who need to be involved at any stage are given adequate opportunity to do so and play an active role in the process and are kept informed of any developments and actions resulting from the process.

2.1. Existing Hazard Identification techniques

Hazard identification is often seen as the heart of risk management. The successful accomplishment of this task is critical since if one omits some potential hazards, it could result in severe human loss and infrastructure damage and in a misevaluation of risk. Many hazard identification techniques [21] have been developed in various engineering disciplines. The precursors of these methods were from the Chemical, Aeronautical and Nuclear power industries. Some methods are area specific such as Hazard Analysis and Critical Control Point (HACCP) for the food industry and others that can be applied to almost any system.

Preliminary Hazard Analysis (PHA) is defined in [19] as a semi-quantitative analysis that is performed to identify all potential hazards and accidental events that may lead to an accident then rank them according to their severity and thereafter identify required hazard controls and follow-up actions. Several variants of PHA are used, and sometimes under different names for instance Rapid Risk Ranking (RRR) and hazard identification (HAZID). The Preliminary Hazard Analysis (PHA) provides an initial overview of the hazards present in the overall flow of the operations of any system. It provides a hazard assessment that is broad, but usually not detailed. The PHA will often serve as the total hazard identification process when risk is low. In higher risk operations, it serves to focus and prioritize follow-on hazard analyses by displaying the full range of risk issues. PHA can be applied to all subsystems, components and systems. Most of the time, it is performed first, prior to or as an initial step of design, operation, maintenance, and refurbishment. PHA is carried out in four main step beginning with PHA prerequisites where the PHA team is established, the system to be analyzed, its components, boundaries and interactions are defined and described as well as the actors or materials that appear to be the most exposed to risk. Next, all hazards and possible accidental events must be identified. In the third step of PHA, the consequence or severity of the hazards in terms of infrastructure damage, human injury or loss is evaluated and frequency of those identified hazards is also estimated. Severity and frequency classification may be used instead when historical risk data is not available to make accurate estimations. Finally, the different hazards are ranked in categories based on their severities and frequencies; this may be done through the application of the ALARP principle [3] explained in Section 3.3. Hazard categorization helps identify which measures and follow up actions should be carried out to remove hazards associated with high risk.

Failure modes, effects, and criticality analysis (FMECA) is a methodology to identify and analyze all potential failure modes of the various parts of a system, the effects these failures may have on the system and how to avoid the failures, and/or mitigate the effects of the failures on the system [19]. FMEA (Failure modes and effects analysis) is a predecessor to FMECA. The C in FMECA indicates that the criticality (or severity) of the various failure effects are considered

and ranked. Today, FMEA is often used as a synonym for FMECA. Although FMECA was one of the first systematic techniques for failure analysis, it is not able to identity complex failure modes involving multiple failures within a subsystem. In other words, it has difficulty identifying hazards that are due to complex interactions of failures. Furthermore it has a limited examination of human error and external influences. FMECA remains the most widely used reliability analysis technique in the initial stages of product/system development, it is usually performed during the conceptual and initial design phases of the system in order to assure that all potential failure modes have been considered and the proper provisions have been made to eliminate these failures.

A Hazard and Operability (HAZOP) study [13] is a structured and systematic examination of a planned or existing process or operation in order to identify and evaluate problems that may represent risks to personnel or equipment, or that may prevent efficient operations. The HAZOP technique was initially developed to analyze chemical process systems, but has later been extended to other types of systems and also to complex operations and to software systems. HAZOP is a qualitative technique which uses special adjectives (such as "more,""less," "no," etc.: being a unique feature) combined with process conditions (such as speed, flow, pressure, etc.) to systematically evaluate deviations from normal conditions. HAZOP also ranks risk based on severity and likelihood and is best suited for the identification of safety hazards and operability problems of continuous process systems, especially fluid and thermal systems and also to review procedures and sequential operations. A major limitation of HAZOP and of the techniques that we introduced thus far is that they focus on one-event causes of deviations.

Multiple-phase failures or hazards due to complex interactions of simple events have to be identified based on the hazards previously identified. Several tools are available for this purpose, including Fault and Event Tree Analysis, Bayesian Belief Networks, Cause-Effect Diagrams and Reliability Block Diagrams.

A Bayesian Network is a directed acyclic graphical representation of the joint probability distribution for a set of discrete variables. To each variable A is attached the conditional probability of A given the parents of A. The graphical representation makes Bayesian networks a flexible tool for constructing models of causal impact between events, in particular when the causal impact has a random nature. Bayesian Networks can be used to model hazards that are the result of complex interactions of simple event.

Cause & Effect analysis (or Fishbone Analysis) provides a structured way to think through all possible causes of a problem, this tool consists of constructing fishbone diagrams, introduced by Kaoru Ishikawa [11] and has been successfully used to track and mitigate several quality problems.

A Reliability Block Diagram [15] is a method of modeling how the components (represented by "blocks") are arranged and related reliability-wise in a larger system and how they combine to cause system failure. Reliability block diagrams may be analyzed to determine the critical components from a reliability viewpoint and can be used to identify multiphase hazards.

Event Tree Analysis (ETA) [3] and Fault Tree Analysis (FTA) [14] are hazard identification methods which are able to implement multiple-phase failures, i.e. deal with complex interactions. According to [3], those two methodologies give rise to a pictorial representation of a Statement in Boolean logic. ETA uses “forward logic”, beginning by an abnormal (initiating) incident or event and propagate it through the system under study by considering all possible ways in which it can affect the behavior of the (sub) system. It takes into account whether installed safety barriers are functioning or not, and additional events and factors. After identifying all potential

accidental events using a PHA, a HAZOP, or some other technique, ETA helps identify all potential accident scenarios and sequences in a complex system. ETA generates qualitative descriptions of potential problems as combinations of events producing various types of problems (range of outcomes) from initiating events. It also produces quantitative estimates of event frequencies or likelihoods and relative importance of various failure sequences and contributing events. This enables giving recommendations for reducing risks and evaluating their effectiveness. ETA is however limited to one initiating event and can easily overlook subtle system dependencies.

On the other hand, FTA uses backward logic, starting from a top event (a potential accident of interest) to seek all the ways it can happen. The analysis proceeds by determining how the top event can be caused by individual or combined lower level failures or events. The causes of the top event are connected through logic gates. Fault trees generate qualitative descriptions of potential problems and combinations of events causing specific problems of interest and also quantitative estimates of failure frequencies and likelihoods, and relative importance of various failure sequences and contributing events. FTA is the most commonly used technique for causal analysis in risk and reliability studies, it has, however, a narrow focus since fault trees zoom on one specific accident; furthermore significant expertise is required for quantification of frequencies.

2.2. Risk Analysis

Risk Analysis consists of the estimation of the frequency of the accidental events and their respective consequences.

The frequency of the accidental events may be estimated based on historical data of previous incidents, fault tree analysis or expert judgment.

The consequence analysis identifies both immediate consequences and those that are not apparent until sometime after the accidental event. All potential event chains following an accidental event must be identified and described. Consequence analysis may be conducted using event tree analysis, simulations or can be derived from historical data. Cause-consequence analysis [6] is another technique for consequence analysis which explores system responses to an initiating "challenge" and enables assessment of the probabilities of unfavorable outcomes at each of a number of mutually exclusive loss levels. This technique provides data similar to that available with an event tree; however, it offers two advantages over the event tree; time sequencing of events is better portrayed, and discrete, staged levels of outcome are analyzed.

It is important to include all consequence categories, these include for the case of level crossing, rail company personnel, passengers, the environment (road side of LC), the economic impact, operational consequences and rail company reputation. Losses may be estimated in terms of human lives, or infrastructure damaged or in financial terms" [5, 20, 22]. Loss of Livelihood should also be included when estimating losses, livelihood being defined as "the command as individual, family or other group has over an income and/or bundle of resources that can be used or exchanged to satisfy its needs" [24].

In the absence of data, one can adopt an ordinal scale for hazard frequency classification and consequence or severity classification. Tables 1 & 2 give possible classifications for hazard frequency and consequence.

2.3. Risk Evaluation

If all the consequences and frequencies of hazards have been identified then quantitative definition of risk can be used to estimate risk:

$$R=\sum R_i \text{ where } R_i = P_i.C_i \qquad (1)$$

Score	Frequency Class
1	Very unlikely
2	Remote
3	Occasional
4	Probable
5	Frequent

Table 1. Hazard Frequency Classification

Score	Severity Class
1	Minor
2	Major
3	Critical
4	Catastrophic

Table 2. Consequence/Severity Classification

In the risk evaluation step, the existing risks are classified and decisions are made regarding the tolerability of the existing risk. Risk tolerability is generally a complicated and multifaceted issue which raises philosophical questions from several angles. Epistemologically one is led to ask: How can we know exactly what a risk is? (Objective vs. Subjective assessment). Ethical and political questions include, for instance, the following: Who should assess the acceptability of a risk? Stakeholders vs. Mathematicians? Another question is about distribution of risks in society whether the distribution is fair? Several principles can be used to determine the acceptable risk:

The precautionary principle [18] is a moral and political principle which states that if an action or policy might cause severe or irreversible harm to the public, in the absence of a scientific consensus that harm would not ensue, the burden of proof falls on those who would advocate taking the action.

GAME or GAMAB meaning “globally at least equivalent” [8], can be applied when looking at either individual or collective risk. This criterion is based on the requirement that the total risk inherent in any new system must not exceed the total risk inherent in comparable existing systems. It is assumed that the risk level of existing systems can be assessed (e.g., using existing statistics). The respective risk levels of an existing system and a new system can only be compared if both systems have comparable performance characteristics and operating conditions.

MEM (minimum endogenous mortality) [8] requires that the total risk from all technical systems affecting an individual must not exceed minimum human mortality (2E-4 deaths per person per year).

ALARP principle [8] ensures that the risks of any system with serious consequences in terms of human loss and injuries, is kept to a level which is As Low As is Reasonably Practicable. ALARP defines three risk levels:

- Intolerable Risk, which cannot be justified or accepted, except in extraordinary circumstances
- Tolerable Risk, which can be accepted only if risk reduction is impractical or if the cost or risk reduction greatly exceeds the benefit gained

- Negligible Risk, which is broadly acceptable and does not require risk mitigating measures

If risk is determined to be at the intolerable level, measures must be taken to reduce it immediately to a tolerable level. If risk is found to be at tolerable level, risk mitigating measures should still be applied, provided that a cost benefit analysis is in favor of it. Table 3 illustrates a risk classification matrix based on ALARP principle.

Frequency/ Consequence	1 Very Unlikely	2 Remote	3 Occasional	4 Probable	5 Frequent
Catastrophic					
Critical					
Major					
Minor					

Negligible Risk Tolerable Risk Intolerable Risk

Table 3. Hazard Categorization based on ALARP principle

2.4. Risk Treatment and Control

Risk treatment is the process of selecting and implementing measures to reduce see remove the risks. Having identified all sources of risks, one will need to prioritize risk treatment actions and target high risk before low risk while maximizing the benefit of the organization.

Two major classes of methods are considered while prioritizing risk treatment actions including Economic Evaluation and Social Evaluation. Social Evaluation is usually used as a prerequisite to the Economic evaluation in decision making as there are a number of factors that cannot be assessed economically. The Economic Evaluation estimates the expected benefits and anticipated costs of control associated with varying degrees of reduction in risk, using monetary criteria which are amenable to quantitative economic analysis. Several types of analysis techniques can be used for economic evaluation of risk treatment alternatives at level crossings including, cost benefit analysis, cost effectiveness analysis and risk benefit analysis [7].

Cost-Benefit Analysis (CBA), also termed benefit-cost analysis or risk-cost-benefit analysis, is a technique that compares for various risk reduction scenarios, the estimated costs of controls put in place against the benefits of the reduced likelihood of accident at LC. This technique calculates the monetized benefit-cost ratio which indicates, when found greater than one (less than one), that projects benefits will likely outweigh the cost of the controls (costs outweigh the benefits). Non-economic considerations should help decide when a risk removal strategy with a benefit-cost ratio inferior to 1 should still be retained. A major difficulty in CBA is that the Costs, Disbenefits and Benefits should be translated into their equivalent monetary value before the benefit cost ratios can be estimated out. It is, however, very difficult to estimate and reach agreement on the economic impacts of benefits and disbenefits for projects intending to put in place controls for risk reduction at LC. Furthermore, a viewpoint must be established (usually after a strong debate in the political arena between different groups) before the economic evaluation. The viewpoint finally adopted will determine the estimates of costs, Benefits and Disbenefits. It should be noted that quantification of the benefits of risk reduction alternatives in monetary terms is an important part of CBA. Various techniques for making quantitative estimates can be used including revealed preferences and stated preferences methods [7]. Revealed preference methods allow an analyst to infer values from actions, for example one

revealed preference method involves measuring prices in benefits in two risk reduction alternatives that are distinguished only by an externality; for example building or not building a bridge to replace a given LC, building a bridge may have an incidence on the economic value of real estate around the LC, this increase or decrease will reflect the monetary benefits or disbenefits of building the bridge to replace the LC. On the other hand, the stated or expressed preference methods consist of using psychometric surveys for asking people about their preferences. They are used especially where no market value actually exists. For example, surveys may be used to ask people of what they are willing to pay to save a human life. This monetary amount can be used to represent what people are willing to pay to increase safety at a LC.

The Cost-Effectiveness Analysis (CEA) technique compares the projected costs for a range of proposed risk control alternatives, all intended to meet the same objective. Although straightforward, this method does not take into account of social and political factors unless they can be somehow converted in monetary value. CEA differs from CBA in that benefits are expressed in physical units (e.g. in LC context, number of life to be saved) rather than in money units. Costs, as in CBA, are expressed in monetary terms. CEA is useful in areas such as health, accident safety and education where it is often easier to quantify benefits in physical terms than to value them in dollars. CEA is useful most often when the benefits of a risk reduction scenario are difficult to quantify in monetary terms but the government wishes to know which option will achieve social benefits or government objectives most cost effectively. One limitation of CEA is that it applies only to situations where all of proposed risk control alternatives are intended to meet the same physical objective.

A Risk benefit Analysis calculates the benefits of the proposed risk control alternatives as a reduction in estimated risk and is not converted to a monetary unit. Risk benefit analysis attempts to define the relation between a given amount of risk reduction (e.g. reduction of frequency of accidents at a LC) and the cost of control measures necessary to achieve it. Risk benefit analysis is frequently the most credible risk management technique when attempting to control high risk situations (e.g. risk of contamination due to transportation of high-risk contaminants). It is wider in scope than the cost effectiveness analysis. A notable advantage of risk benefit analysis is that it does not require the conversion of the benefit into monetary measures. It requires, however, a prior determination of what an acceptable level of risk is.

A major component of risk treatment is risk control which consists of putting in place control mechanisms to make sure that risk is permanently removed/decreased.

2.5. Monitoring and Reviewing the Risk Management Process

Monitoring and review of the risk management process is a mean to make sure that the actions taken effective and that the procedures adopted and information gathered throughout the process were appropriate. It should be noted that systems are evolving which means that they may get exposed to new risks as they evolve over time, reviewing and monitoring enable keeping track of the changes that systems may undergo.

3. Global Safety Management System in the Railway Sector

3.1. Definition of a Safety Management System

Safety management is an important issue in all safety critical sectors including railway industry and regarded as an important means for improving safety culture.
A safety management system (SMS) [2] is an organization's formal arrangement, through the provision of policies, resources and processes, to ensure the safety of its work activity. An effective SMS helps the organization to identify and manage risks effectively. It allows an organization to demonstrate its capability in achieving its safety objectives and in meeting regulatory requirements. A crucial aspect of safety management activity will be the management of interfaces. The number of interfaces has increased significantly due to the liberalized rail transport and new organizational structure worldwide and in Europe in particular.

3.2. Safety Management System and Lifecycle Stages of the Railway Transport System

The main lifecycle stages of a Railway Transport System have been discussed in European norms [8] and other similar documents, a schematic view of this is presented in Figure 2.

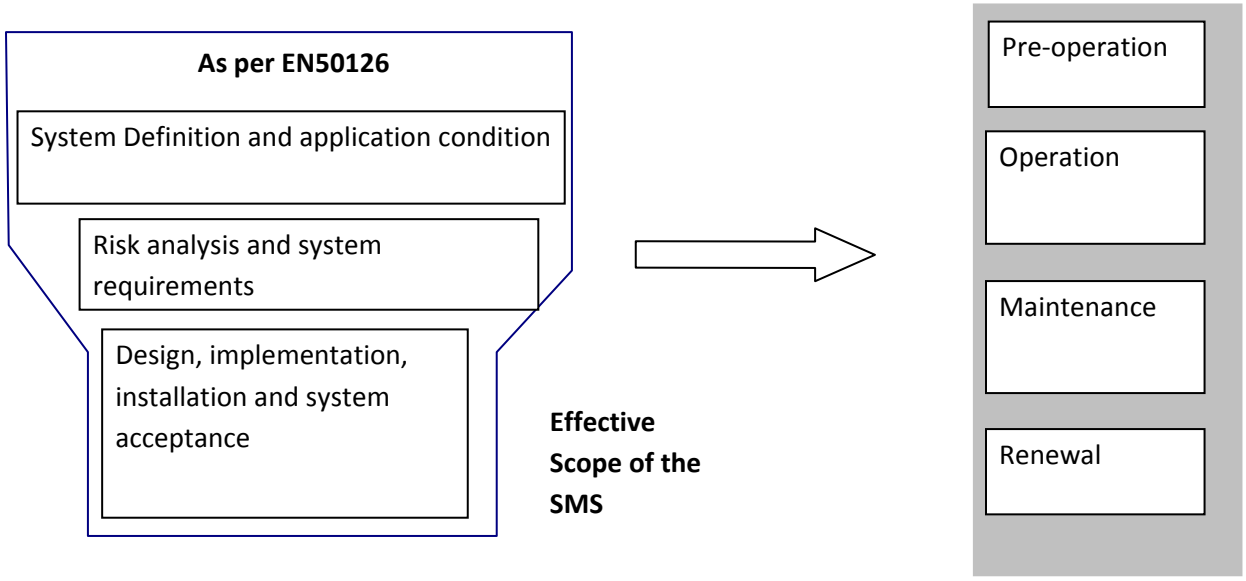

Figure 2: Appropriate SMS guidance for each lifecycle phase

Mainly, the SMS framework focuses on generic management issues. Its actual effectiveness very much depends on how this framework is applied to the specific business processes related to the systems, subsystems and equipment the duty holder controls. There should be specific elements of any developed SMS that deal with aspects of each of the following stages of the Railway Transport System lifecycle:

- Pre-operation: Safety approval, system handover and acceptance are therefore crucial interfaces between the developer and the duty-holder that need to be managed effectively to ensure safety. The duty-holders need to assure themselves that the system development has been undertaken in a manner that is consistent with the risk tolerability criteria set for this overall Railway Transport System SMS framework. This assurance will be supported by

evidence of application of a robust development process such as that described in safety CENELEC standards or equivalent [8, 9]. This approach implies that the developer should be aware of the risk tolerability criteria. The duty-holder must also assure itself that the overall system, within which any procured element is to be used, remains safe. Each duty holder should have in place necessary arrangements for accepting new components. This should ensure that only 'operationally ready' equipments, subsystems or systems are accepted for operational usage. The acceptance criteria used for such purposes should comply with EU and national requirement, and their integration and commissioning procedures with the Railway Transportation System should be identified.

- Operation: The duty holder should have the necessary arrangements for identifying the operating requirements of the equipment, subsystems and systems it controls. They should include requirements and constraints for their normal and degraded modes of operation. Generally, regulations, rulebooks and work procedures provide detailed instructions for performing critical operations. The duty holder organization should specify how these rulebooks are to be developed, how the rules will be formulated, written and approved; how the use of rules will be monitored and, where appropriate, how the rules will be enforced or modified and maintained to improve their performances.
- Maintenance: A duty holder should have adequate arrangements for implementing planned and preventative maintenance (including, where appropriate, maintenance based on monitoring of equipment condition) of its equipment, subsystems and systems. All such items should be identified, prioritized in terms of frequency and standard of maintenance and adequate resources identified to meet the maintenance schedules. The procedures for removing items from the operation and for preparing them for maintenance should be identified. Similarly, procedures for commissioning and accepting repaired items for operational use should be identified.
- Renewal: A duty-holder should have necessary arrangements for identifying and planning renewal work which it has to undertake for regulatory or business reasons. For example, for maintaining performance level a duty holder may need to carry out like for like replacement for time-expired assets, or introduce new technology to improve performance. There should be procedures for monitoring critical items and preparing plans for their timely replacement.

A key source of risk is at the transition between lifecycle phases, e.g. the resumption of operations after a period of maintenance. Lifecycle transition should be explicitly addressed in risk assessment activity. It is assumed that all the concerned work places, e.g. operational area, maintenance depot and project site should be subjected to required Health and Safety at Work regulations.

3.3. Integrating the suggested Risk Management Framework into Railway Safety Management System

Table 4 shows the proposed eleven elements of the SMS that are divided into two parts: Planning and risk control system and learning system. This organization of SMS structure should be refined at Stakeholders level and should consider the operation, maintenance and renewal phases of the life cycle [8] of the railway system and lifecycle transition should be explicitly considered in risk assessment activity. The risk management framework for railway sector which we suggested in Section 2 can be integrated in element (5) of a SMS.

Planning and risk control system	*Learning system*
(1) Nature and Scope of Duty Holder's Business	(10) Incident and Accident Reporting and Learning
(2) Safety Policy	
(3)Organisational structure and Responsibilities	(11) Monitoring, Auditing, Corrective Measures and Annual Reports
(4) Competence, Training and Fitness	
(5) Risk Management	
(6) Safety Assurance	
(7)Emergency Management	
(8) Safety Communication and Information	
(9) Management of Rules and Standards, including Compliance	

Table 4: Structure of Safety Management System

4. Risk Assessment for Level Crossings: Application to a Moroccan Level Crossing

4.1. Description of the system under study

A level crossing (LC) is an intersection between the road and the railway that allows vehicles of any type to pass through it. The "danger zone" is the area of the intersection in which a collision between the incoming train and LC road users (vehicles and pedestrians crossing the LC) can take place. LCs differ in the protection they offer users, their degree of usage, and in the speed and frequency of the trains that pass over them. LCs are categorized into active crossings where the road user is given a warning of incoming train or passive crossings where no warning is provided, the responsibility being on the road users to determine whether it is safe to cross the LC. Moreover, active LCs can be split into two major subcategories i.e. manual and automatic LCs. In Morocco, the only type of active LC used is the manually controlled full-barriers (MCB) which will serve as the basis of our risk assessment study. The Moroccan LC studied is composed of two rail tracks, and is crossed by a two-way road. The LC is operated by a LC keeper who is responsible for lifting and lowering the mechanical full-barriers and also for alerting the different LC actors of the presence of danger at the LC.

Technical characteristics of the Moroccan Level Crossings

The Moroccan national railway organization, ONCF, classifies its LCs according to two criteria, namely LC moments and their location. The LC moment corresponds to the number of trains and vehicles (cars and motorcycles) that pass through the LC in a 24 hours period:

$$\text{LC moment} = [\text{Number of trains / 24h}] * [\text{Number of Vehicles / 24h}] \qquad (2)$$

The second criterion, which is related to the location of the LC, corresponds to the visibility of the incoming train by the vehicles drivers. In fact, ONCF defines a sufficient visibility when a person being at 5 meters from the nearest rail track and whose eye is at one meter from the ground sees the complete locomotive (railway engine used to tow railway cars), moving at the maximum authorized speed, for a period of 20 seconds.
The ONCF classifies LC with a moment in the interval [2000, 5000] and insufficient visibility as first category. These first category level crossings are manually controlled barriers LC and are the subject of our study.

Railway signaling: The railway signals include:

- A metallic announcing panel made out of light-sensitive tapes representing a barrier with the LC number at the top of it. This panel is placed before and after the LC at a distance of 700 m when the authorized train speed does not exceed 120 km/h and at 800 m when this speed is greater than 120 km/h.
- An « S » panel placed at 300 m before and after the LC to remind the train driver that he should whistle to alert both the LC keeper and the vehicles passing through the LC of its incoming.
- White-painted pylons located at least at 500 m before and after the LC

Road signaling; There exist two types of road signals, advanced signals and position signals:

- The Advanced Signal is a triangular panel A9 placed at 150 m from the LC which informs the road users that they are approaching a MCB LC and that they should decelerate and be cautious at the LC.
- Position Signals are barriers with tapes of 1 meter length each painted in red and white.

Incoming Train Detection System-Electro-Mechanical Detection: ONCF is using Electro-Mechanical oriented pedal in all Train Detection System (TDS) at manned LC. This automated TDS is composed of pedals placed at the middle of each rail track of the railway 3000 m from the LC. The TDS is directly connected via electrical wires to the LC's control board and when activated the TDS will trigger both the audible and visual signals at the LC, indicating the direction of the incoming train. These devices are installed in a box located at proximity from the LC Keeper's shelter and the barriers so that the LC keeper can hear and see it perfectly. When the train passes on the rail track, it activates mechanically the pedals, then the road signal changes from green to red. The incoming train's audible announcement can only be turned off if both the LC keeper deactivates the system by pushing on a button on his control board and the pedal is no longer active, train passed the location of the pedals.

Entities Involved in the Moroccan manually controlled full barriers crossings: Several entities may impact the normal operations of the MCB crossings, including the condition of the railway, the condition of the road crossing the railway, the condition of level crossing mechanisms, the train detection system, the transmission/communication system, the road signaling, the railway signaling and the level crossing human actors which include the train driver, the level crossing keeper, the road user and the control center operator.

Modeling operational interactions at the LC through functional diagrams: Many of the existing hazards at LC may be due to operational failures which can be identified by building functional diagrams representing the LC from different perspective and then identifying operational conditions which may lead to accidents. These functional diagrams give a visual representation of the sequence of events and interactions between the different entities involved in the LC operations and enable a detailed functional understanding of the system. For this purpose we built functional diagrams, for the LC under study, from the perspectives of the different actors in the LC including the LC keeper, the road user, the train driver and control center operator.

4.2. Hazard Identification at MCB Moroccan LC

In order to identify the complete set of hazards surrounding the MCB LC under study, we considered the different entities involved in the LC and the interactions between them described by functional diagrams. We also reviewed the operational specifications and considered all the environment factors around the LC. We considered the human and LC interface. We identified several hazards that can be classified into one of five categories, namely hazards related to the environment of the LC which affect visibility of LC users, hazards related to technical problems, hazards due to non compliance with standards, hazards due to the human factors, and the fifth category includes all the other hazards. Several sub-categories constitute each hazard category. After several brainstorming sessions, we identified 63 potential hazards along the five hazard categories. We present in Table 5 a sample of the identified hazards.

HAZARDS
Improperly closed gates when the train passes through the LC
Road vehicles coming over the LC where barriers on the other side have been closed
Drivers disregarding signals
Low level of public discipline
Technical Malfunction of a vehicle that makes it stop in the middle of the railway track while a train is coming towards the LC
Poor road surface state causing the crossing of vehicles difficult
Non-Compliance of road standards by the road authorities

Non-Compliance of railway standards by the railway authorities
Poor Maintenance of LC
Barriers take too much time to close and some vehicles cross the LC while the train is near by
Restricted Visibility of the Road signals by the drivers (due to the presence of physical obstructions)
Restricted Visibility of the railway signals by the train driver (due to the presence of physical obstructions)
Restricted Visibility of the Incoming Train (large turn angle or angle of the road)
Elevation of the road crossing the track that makes the car stall
Absence of Road Warnings and Signals
Motorcycles' Drivers ignore signals and pass under the closed LC barriers
Light Signal is not working and do not alert both the LC keeper and its users
Non luminescent barriers (of use at night)
Train brakes do not work
Non-activation of the detection system & Train Alarm does not work
Car Drivers try to cross while the train approaches and the barriers are being lowered
Traffic jam at the level of the LC while a train is coming towards the LC
Signal Transmission between the activating arm of the TDS and the LC Control Board fails due to poor maintenance
Non-activation of the audible and light signals by the Train Detection System
Inaudible Alarm of the train that is meant to alert the LC keeper of its incoming

Table 5. A sample of the hazards identified for the MCB under study

The pie-chart in Figure 3 illustrates the distribution of the hazards identified by category. According to this chart, the hazard categories, "Human Factors" and "Technical Problems", with respectively 37% and 29% of the overall system hazards identified, are the two major hazards that can lead to an accident at the MCB LC. Therefore, a detailed analysis of both categories was needed to understand and identify which actors (people or sub-system parts) are responsible for the majority of them and to state if some actions can be undertaken by the appropriate authorities to reduce their impact, as a future step.

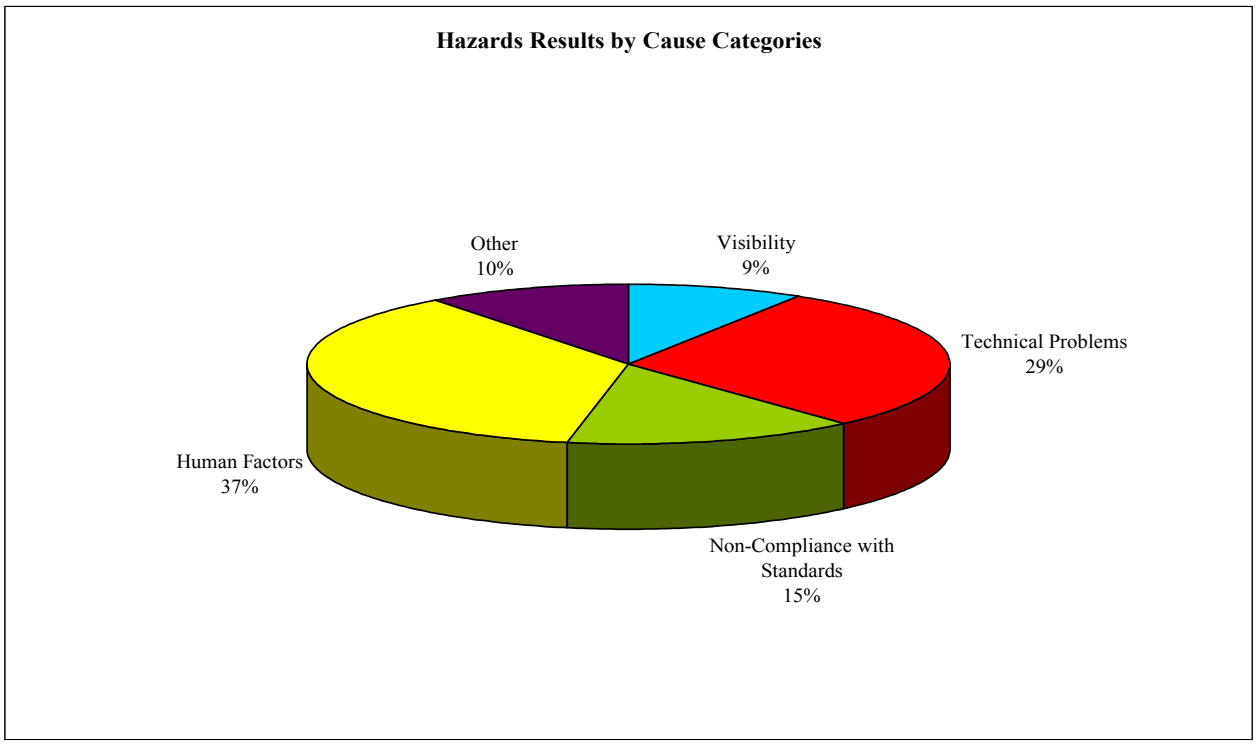

Figure 3. Hazards Identification Results classified by cause categories

4.3. Risk Analysis, Evaluation and Treatment at the MCB Moroccan LC

Since we did not have historical data for risk analysis, we used the frequency and consequence classification described in Tables 1 & 2 to rank each of the 63 identified hazards and then categorized them based on ALARP principle as explained in Table 3. This revealed that 18% of the hazards are considered to have negligible risk, 35% have tolerable risk and they include mainly technical problems related to the train and the TDS. The remaining 47% hazards were associated with the intolerable risk category, and most of them were associated with the human factor and technical problems. The next logical step is to take actions to remove hazards with potential intolerable risk. These actions should target human factors and technical problems.

5. Conclusion

In this paper, a framework for risk management at railways has been introduced and integrated into global safety management system of railways. Furthermore we illustrate how it was applied to a manually controlled full barrier road rail level crossing in Morocco. We suggested different aspects that should be considered during the system definition phase where we suggested using functional diagrams for modeling operations at LC from the perspective of LC actors. It is a critical part for risk management and specifically for hazard identification where we provided different techniques that can be used; our experience shows that involvement of all stakeholders is a prerequisite to the success to this phase. Initiating events can be unveiled through brainstorming sessions and FTA can model complex interactions of events that have the potential to lead to accidents. Risk analysis can then be carried out provided that historical LC accident

and incident data is available to estimate frequencies and consequences; ETA is the ideal tool for estimating consequences of hazards due to multiple causes. The existing risks are then classified and decisions are made regarding their tolerability, the ALARP principle can serve this purpose. A cost benefit analysis then helps prioritize risk treatment actions that should target intolerable risks. Control mechanisms should be also put in place to assess, monitor and review the risk control actions put in place. Finally, we emphasize on the importance of having a database of historical accidents and incidents at LC for the success and efficiency for the suggested framework.

Acknowledgements:

This work is conducted within SELCAT project funded by European commission and we would like to thank all project partners.

References:

[1] AS/NZS 4360. Risk Management. Standards Australia, Sydney, 1999.

[2] G. Bearfield, S. Mitra, and E.M. El Koursi, "Guidelines for Safety Management System, D2.2.2/V3.0", http://samnet.inrets.fr, May 2004.

[3] T. Bedford, and R. Cooke, "Probabilistic Risk Analysis – Foundations and Methods", Cambridge Press, 2001.

[4] B.S. Blanchard, "System Engineering Management". John Wiley & Sons, New York. 1998.

[5] I. Burton, R. W. Kates, G.F. White, "The Environment as Hazard", Second Edition, Guildford Press, New Yord/London, 1993.

[6] A. Clifton, I.I. Ericson, "Hazard Analysis Techniques for System Safety", John Wiley & Sons, 2005.

[7] Commonwealth of Australia, "Introduction to Cost-Benefit Analysis and Alternative Evaluation Methodologies", January 2006.

[8] EN 50126: "Railway applications—The specification and demonstration of reliability, availability, maintainability and safety (RAMS)." CENELEC, 1999.

[9] CENELEC: EN 50129 "Railway Application: Safety related electronic systems for signalling", February 2003.

[10] "The Risk Management Standard". Published by the Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) and ALARM in 2002. www.theirm.org/publications/PUstandard.html

[11] K. Ishikawa, "Guide to Quality Control", 2nd rev. ed. Available from UNIPUB/Quality Ressources, One Water Street, White Plains, NY 10601. Tokyo: Asian Productivity Organization, 1986.

[12] S. Kaplan, and G.J. Garrick, "On the quantitative definition of risk, Risk Analysis", vol 1, no. 1. 1981.

[13] T. A. Kletz, "Hazop – past and future". Reliability Engineering and System Safety, 55, pp. 263-266, 1997.

[14] WS. Lee, DL. Grosh, EA. Tillman, CH. Lie. "Fault tree analysis, methods and applications—a review". IEEE Trans Reliab ;R-34(3), pp.194–203, 1985.

[15] L.M.,Leemis, "Reliability - Probabilistic Models and Statistical Methods", Prentice Hall, Inc., Englewood Cliffs, New Jersey, 1995.

[16] M. Modarres, "What Every Engineer Should Know about Reliability and Risk Analysis". Marcel Dekker, NewYork. 1993.

[17] V. Molak, "Fundamentals of Risk Analysis and Risk Management". CRC Press, Lewis Publishers, Boca Raton, 1997.

[18] C. Raffensberger, J. Tickner, "Protecting Public Health and the Environment: Implementing the Precautionary Principle". Island Press, Washington, DC, 1999.

[19] M. Rausand, and A. Høyland. "System Reliability Theory; Models, Statistical Methods and Applications", Wiley, New York, 2004.

[20] E. Schnieder, R. Slovak, and S. Wegele, "New and Conventional Measures for Quantifying Risk in Rail Transport". Journal of System Safety, February 2005.

[21] MG. Stewart, RE. Melchers, “Probabilistic risk assessment of engineering systems”. London: Chapman & Hall, 1997.
[22] United Nations Disaster Relief Coordinator, “Natural Disasters and Vulnerability Analysis”, in Report of Expert Group Meeting, UNDRO, Geneva. 9-12 July 1979.
[23] J.X. Wang, and M.L. Roush. “What Every Engineer Should Know About Risk Engineering and Management”. Marcel Dekker, New York, 2000.
[24] P. Blaikie, T. Cannon, I. Davis, B. Wisner, “At Risk: Natural Hazards, People's Vulnerability, and Disasters”. London: Routledge, 1994.