9

# A Systems Approach to Assurance of Safety, Security and Sustainability in Railways

A.G. Hessami
*Innovation Director, Vega Systems*
*UK*

## 1. Introduction

The transportation network constitutes the artery of economic activity and growth in modern economies. Whilst challenged by telecommunications and internet technologies, the movement of goods and people is still an indispensable aspect of social and economic life contributing around one tenth of the GDP in the developed world economies[1]. It is not surprising therefore to find transportation on the social and political agenda and any faults, failures and consequent accidents, being given a high degree of publicity and exposure. Traditionally, the key mantra in transportation especially railways has been safety followed by reliability, punctuality, cost, journey time and quality of travel. This has held true so far for most modes of transport until recently when malicious intent with the aim of disrupting the network, victimising its customers and inflicting large economic losses has added a new ingredient to the traditional concerns of the industry. The malicious intent broadly falls into a number of categories comprising;

- Vandalism & Unlawful Adventure
- Robberies, Assaults
- Illegal Access
- Unauthorised Use of Property/Facilities
- Theft, Fraud
- Intimidation and Extortion
- Disruption, Sabotage
- Terrorism

Whilst vandalism is of limited consequence and often related to adventure seeking youth, the other categories of concern specifically terrorism pose a largely new sinister development often beyond the powers of transportation authorities to predict, prevent or contain. This is where the power of scientific structured approaches and methodologies principally applied in safety engineering can be exploited to render assurance in integrated transportation safety and security in Road, Rail, Shipping and Aviation including the Transport Hubs.

[1] U.S. Department of Commerce, Bureau of Economic Analysis

The rapid development of technology generates new products, systems, services and process knowledge often with significant potential to improve technical, commercial and environmental performance and enhance the overall quality of life. However, the new innovations especially those with embedded intelligence and adaptability are plagued by uncertainty about their overall characteristics including the concern about the risks arising from their adoption. To this end, a systemic assurance process and associated methodologies are required to underpin verification, validation and enhanced confidence in the desired performance of industrial & technological systems and innovations.

With the advent of high-speed rail transportation technology, the industry is now poised to compete with short haul aviation and deliver enhanced economic and social benefits across the world. The technology that was first introduced in Japan in the 1960s is now advanced and pervasively employed in much of Western Europe, South East Asia and the People's Republic of China. As a notable case, China that currently boasts a standard and high speed rail network of 53000 miles plans to spend an estimated $300 billion to meet a 2020 target of 75000 miles with the world's largest high speed network (Green Leap Forward, 2010). In spite of high economic cost, there are a number of compelling reasons in favour of high-speed rail namely incessant demand for mobility, accelerated economic development and more sustainable transport using electric trains. Whilst high speed rail networks are deemed to transform economic geography by bringing cities closer together, enabling higher business productivity, supporting employment growth and regeneration, the inherent complex technologies adopted require extensive scrutiny, verification and assurance to ensure desirable levels of safety, security and potentially higher attained sustainability.

### 1.1 Background

Aided by the transportation, communications and computer technologies, the global village presents many opportunities and benefits to mankind from rise in international trade and growth to redistribution of wealth. However, alongside these emerging opportunities, innovations, scientific discoveries and burgeoning complexities in products, processes and indeed human relationships pose a challenge to mankind threatening health, safety, security and the natural habitat. In a recent international survey, DEMOS the think tank organisation (DEMOS, 2007) identified six major global drivers for change namely:

- Pervasive Complexity;
- Matrix versus Functional Restructuring;
- Riskier Markets;
- Transition to Knowledge Economy;
- New Business Practices, Offshoring & Outsourcing;
- New Accountabilities, Corporate Governance and Corporate Social Responsibility.

Prudent exploitation of the opportunities and credible assessment/management of potential adversities in the face of these influential drivers demands a more systematic and potent approach to tackling the emerging global challenges.

### 1.1.1 Safety

Safety is synonymous with freedom from unacceptable levels of harm to people and is a highly desirable property of products, systems, processes and services. However, in view of ever increasing complexity, faster pace of development and change, safety is often difficult if not sometimes impossible to entirely predict, manage and guarantee. At the same time, rising social awareness and the more stringent legal requirements almost globally demand higher levels of safety performance from products, processes, systems, services and the duty holders. Safety problems are characterised by unintended yet harmful incidents and accidents that apart from acts of nature are mainly traceable to our shortcomings in concept, design, development, deployment or maintenance of products, systems and services. Safety is heavily regulated and health, safety and welfare of people are under legal protection in most developed and increasingly in developing countries.

### 1.1.2 Security

Security is synonymous with freedom from unacceptable levels of harm to people, damage to business operation/property or the natural habitat. Unlike safety, security problems are characterised by often malicious intent (threat) which aligned with inherent or intrinsic vulnerabilities cause incidents and accidents with significant potential to cause harm and consequent loss. However, complexity, rapid change, global geopolitics and novelty pose increasing threat to the security of products, processes and systems requiring an enhanced degree of proactive assurance. Security, as yet, is not generally regulated and freedom from intentional harm to people and property is still largely a commercial decision by duty holders.

### 1.1.3 The Environment & sustainability

Since the dawn of industrial revolution, the scale of mankind's influence on the natural habitat has increased significantly. Apart from the depletion of non-renewable resources and generation of waste and heat, industrial and man-made disasters often involve the natural environment causing damage, contamination or major change in the ecology to the detriment of plants, wild life and potential for human habitation. Given man's destiny and quality of life on the planet are strongly related to the health and balance in the natural habitat, the environment is now protected through regulation enforced through laws and government agencies.

### 1.1.4 Synergies

Safety and security possess a significant synergy in that safety is characterised by unintended and security by intended errors, faults, failures and acts leading to accidents. Apart from differences arising from the nature of intent, the prediction, prevention and successful risk control in both contexts can be carried out in one integrated regime due to similarity of escalation processes and much of remedial actions. The concurrent identification, assessment and mitigation of safety, security and environmental issues render enhanced integrity whilst posing significant savings in costs and time scale for assurance on these fronts.

The regulatory regime is the key instrument in the overall certification and deployment of new innovations in products and services. Many developments including the safety case regime mandated within nuclear, offshore (Offshore Safety Case Regulations, 2005) and rail

transportation (Railway Safety Case Regulations, 2000) in the UK are intended to pave the way to enhanced confidence as well as rapid deployment of modern innovations. In this context a systematic and principled approach to identification, control and management of risks is fundamental to the achievement, maintenance and improvement of the overall confidence and performance of products, processes, services, systems and undertakings.

Products, processes and systems exhibit a number of facets in their performance that are either inherent or perceived by the relevant stakeholders. These generally comprise:

a. Technical/operational;
b. Commercial;
c. Safety & security;
d. Environmental & sustainability;
e. Reliability, availability & maintainability;
f. Quality;
g. Perceived value.

Amongst these often inter-related aspects of performance only safety and environmental dimensions of products, processes, services and systems are currently subject to regulation (Hessami, 2004). Understanding the key factors influencing the overall safety and security performance of various services, industrial and infrastructure systems will lead to the development of policy initiatives to promote safer, more secure and cost-effective solutions at the enterprise and industry level. It will also simplify regulation while providing transfer of knowledge and expertise from more successful domains and states to those that have evolved at a slower pace. With the advent of high-speed rail transport, the industry requires higher degrees of confidence and assurance in the advanced products, systems and services deployed to avoid costly accidents. To this end, a systematic framework for identification, evaluation, assessment and management of risks founded in systems theory is called for.

## 2. Risk and assurance

### 2.1 Derivation of principles

A principle is regarded as a fundamental truth or proposition on which many other propositions depend. It is also regarded as a fundamental assumption forming the basis of a chain of reasoning. It is argued that a management regime founded on a suite of principles will be superior in terms of its stability, integrity, effectiveness and its capacity to be adaptable and scalable for multiplicity of circumstances and stakeholders since it is constructed using a set of fundamental & universal truths. A framework for management of risks should inherently address all life-cycle phases and issues comprising:

- Definition and characterisation of the system of concern and its environment of application;
- Identification/recognition of fundamental threats, faults and failures (causes of hazards);
- Prediction of realisation/occurrence of hazardous states arising from threats, faults and failures;
- Assessment of potential escalation of hazardous states into accidents/loss scenarios;
- Coverage of post-accident scenarios, actions and recovery processes;

- Human organisation, capabilities, resourcing, procedures and competencies;
- An inherent monitoring, measurement and enhancement regime.

On the other hand, assurance is synonymous with gaining increasing confidence about the performance of an often complex product, service, process or system so that;

- It delivers an optimal level of essential and desirable properties/performance
- It is free form an unacceptable level of undesirable properties/performance

A systems framework based on a complete and inter-related set of principles for performance assurance would enhance the degree of confidence that apart from the delivery of required functionality, the product, service, process or system is free from potentially harmful properties and behaviours hence assurance.

A key aspect of the current approaches to understanding and managing desirable and undesirable properties is the disjointed and unsystematic treatment of the issues in these domains (Hessami, 1999). Apart from lack of joined up approach in even one of these domains, most experts operating in one domain operate independently often unaware of the issues, processes and solutions in the other.

It is argued that a comprehensive scrutiny, objective evaluation, assessment, understanding and management paradigm encompassing a systems world view would result in enhanced assurance and surety, in the face of complexity, uncertainty and change.

## 3. The systems approach

We propose two complementary and advanced sets of systemic principles and processes as the underpinning backbone to tackling the challenges of safety, security and sustainability in all products, processes, services, systems and undertakings. This is particularly pertinent in the modern railway environment in view of the pervasive deployment of advanced technologies to deliver higher speed and improved efficiencies. Taking a life-cycle perspective, these comprise items I and III below;

i. Assessment: This comprises proactively recognising the need, defining the system, specifying and identifying/understanding of key properties, behaviours, hazards and vulnerabilities, evaluating and assessing expected impact;
ii. Realisation: This is ultimately aimed at developing the product, process, system, mission or undertaking whilst incorporating the desirable properties and avoiding the undesirable behaviours thus achieving the optimal performance;
iii. Management: this comprises taking the outcome of assessment and realisation into consideration and ensuring deployment, delivery of requisite performance, continued monitoring and control through a responsive and holistic suite of strategies and actions.

Whilst Realisation is specific to a given domain, context and technology, the Assessment and Management aspects as a suite of principles constitute a meta-knowledge framework that can be abstracted and developed for almost universal application across many domains and disciplines. The systemic framework of assessment and management is equally applicable and effective within the context of desirable as well as undesirable properties of products, services and systems. This is contrary to the current conventional wisdom where specification, delivery and continual monitoring of desirable aspects of performance is

regarded as an essentially domain expertise whereas the undesirable and unintended emergent properties (hazards and vulnerabilities) are the forte of so called risk management. The +Safe3 extension (Australian Defence Materials Org, 2007) to the renowned CMMi model (Chrissis et al, 2007) also distinguishes between Safety Engineering & Safety Management, which are mainly synonymous with Risk Assessment and Risk Management advocated here.

Whilst presented as a dual and complementary suite of principles and processes, assessment and management are iterative and systemic in the sense that processes inherent in the management framework employ assessment activities at requisite points to support judicious decision-making and ensuring optimal performance. These are collectively referred to as Systems Assurance and labelled as Surety Framework.

### 3.1 Risk assessment

This key facet of Surety framework depicted in figure 1 is proposed as a backbone to the identification, specification, evaluation and assessment of the undesirable events or properties adversely affecting technical functionality, cost, reliability, safety, quality etc. The risk assessment process (Railtrack plc, 2000) comprises seven systemic aspects such as:

a. Hazard Identification;
b. Causal Analysis;
c. Consequence Analysis;
d. Loss Analysis;
e. Options Analysis;
f. Impact Analysis;
g. Demonstration of Compliance.

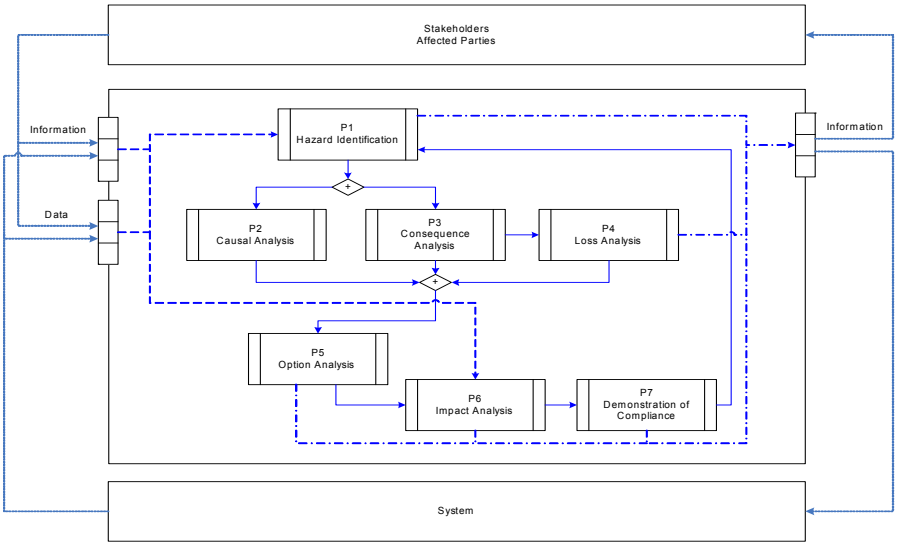



Fig. 1. The Systematic Framework for Risk Assessment, its interfaces and interactions

The principles of risk assessment are general and equally applicable to the qualitative as well as the quantitative approaches to this discipline. They constitute a systematic framework within which, a broad spectrum of situations hazardous to health, safety and security of people and detriments to the environment or an enterprise may be identified, analysed and assessed.

The qualitative risk assessment process broadly relies on expert judgement and empirical experience sometimes within a subjective and coarse quantitative process. It is worth noting that mere use of quantification and numbers does not necessarily qualify an assessment as quantitative. These are however mainly a reflection of judgement and lack the objectivity and accuracy to generate a detailed and reliable measure of risks.

The Risk Assessment process highlighted above satisfies the following requirements;

- Potential for use of modelling;
- Predominate application of objective and validated data;
- Treatment of uncertainty associated with input data and results;
- Treatment of dependency between significant factors;
- Use of statistical simulation where appropriate.

Modelling predominately represents a simplification and generalisation of reality but, enhances our understanding of causal relationships, highlights important factors and provides a useful tool for anticipation and potentially prediction of future.

**Advantages**

The quantitative framework for assessment of risks arising from hazards of undertakings, services, products and processes, yields a number of major advantages over its qualitative counterpart;

- generates a quantified measure of risks in complex situations;
- capable of addressing uncertainty and statistical variations in input data;
- capable of addressing dependencies in the input parameters/data;
- capable of generating confidence intervals for the quantified risks;
- capable of demonstrating compliance with ALARP and other Industry Benchmarks;
- auditable objective process with scope for review and improvement;
- does not employ arbitrary tolerability criteria popularised by risk matrices;
- does not require customisation or a specific form of a ranking matrix;
- provides an auditable and traceable approach to decision support;
- employs the same framework and principles as in the qualitative approach.

**Disadvantages**

The constraints and dis-benefits of the quantitative approach must be borne in mind however, namely;

- complex hence unsuitable for low risk systems and undertakings;
- requires expert resource in knowledge elicitation and risk modelling;
- need for extensive range of objective data and the requisite pre-processing;
- need for formidable computing resource and know-how;

- resource intensive, costly hence inappropriate for applications where a qualitative approach may suffice;
- lack of readily available, robust and comprehensive computer based tools.

The quantitative approach to assessment, recording and management of risks strives to generate a systematic framework for decision-making and demonstration of legal and professional duty of care. In contrast with the qualitative approach and in compliance with the spirit of the Safety Case regime (CENELEC, 2003) and Regulations, the approach and methodologies of the quantitative process are more stringent and thus germane to the nature of significant risks.

The systems framework comprising seven key principles highlighted above is equally applicable to qualitative and quantitative approaches to the assessment of risks arising from products, processes, services, undertakings and systems. The guidance for the required processing at each one of the seven stages of the systematic risk assessment framework is given below, commensurate with the requirements of the quantified process.

### 3.1.1 Hazard identification

Circumstances with a potential to lead to loss, i.e. harm to people, financial detriment or environmental damage are associated with most activities and undertakings. Whilst it is relatively straightforward to identify these within the context of familiar day-to-day tasks and experiences, more complex products, processes, services and undertakings generally pose a more arduous if not insurmountable challenge in this respect. Rapid development and widespread exploitation of cost saving or performance enhancing technologies generally exacerbate the situation and increase the scope for larger potential losses in the event of unforeseen or unprotected errors and failures.

The structured comprehensive identification of hazardous circumstances arising from threats or unintended failure of products, services, systems, processes or human error/action is fundamental to any safety and security process. It is however even more pertinent to large scale or complex undertakings with a potential to lead to significant losses in the event of hazardous occurrences. In the absence of a systematic and robust hazard identification phase, all the subsequent safety analysis processes amount to no more than an exercise in vain, creating an illusion of safety/security and a false sense of confidence and comfort. This is particularly pertinent to circumstances where, due to a poor process, a number of significant hazards remain un-identified hence dormant within the system posing intrinsic vulnerabilities.

The determination of the domain of influence of a product, process, service or undertaking is another by-product of the systematic hazard identification process. This is essential in establishing the scope of the subsequent assessment and should be employed in preference to the traditional approach based on the physical boundaries of the subject under consideration. The radiation of electro-magnetic interference typifies instances where the domain of influence extends well beyond the physical boundaries of a poorly designed and constructed system.

The systematic identification of hazardous circumstances entails two key stages at the outset;

- Empirical Phase;
- Creative Phase.

In view of the extensive resource requirements, the approach described here is more appropriate to products, services, processes and undertakings that are likely to lead to significant losses due to their scope, scale or novelty.

#### 3.1.1.1 Empirical phase

Traditionally, the knowledge and experience of the past, in the form of Check-lists have been applied to the determination of the potential hazardous circumstances in new products, processes and undertakings. This approach is seldom adequate in isolation especially, when there are novelties or significant changes in the functionality, technology, composition, environment (time / space) or the mode of exploitation of the matter under consideration. It is essential therefore to compile and maintain a Check-list of hazardous circumstances pertinent to specific products, processes or undertakings, in order to facilitate a simple first cut identification of the likely problem spots and where possible, avoid the errors, failures and losses of the past.

Where the product, process or undertaking lend themselves to a more detailed scrutiny, Failure Mode and Effects Analysis (FMEA) for equipment / systems and its human related counterparts, Action Error Analysis and Task Analysis may be applied in order to identify the particular component failures or errors conducive to hazardous circumstances. These however require a detailed knowledge of the failure modes of the components and sub-systems, including human actions and the likely errors.

The application of Check-lists, FMEA, Action Error Analysis and Task Analysis are generally not resource intensive and may be carried out by suitably competent individuals and appropriately recorded for further analysis. The hazards identified through the application of these techniques generally constitute a sub-set of the total Potential Hazard Space that should be further explored with the aid of the complementary Creative techniques.

#### 3.1.1.2 Creative phase

The systematic and creative techniques have an established pedigree in the analysis and resolution of complex problems. These generally capitalise on cognitive diversity through a team based approach, comprising members with diverse and complementary knowledge and backgrounds. Furthermore, in view of their reliance on lateral perception, divergent thinking and imaginative creative faculties, the structured and systematic variants of these techniques generally share a numbers of key characteristics namely:

- planning and process management;
- study panel (team) selection and briefing;
- hierarchical decomposition and graphical representation of the problem domain;
- high level probing of the key elements of the system and coarse determination of the critical sub-systems and interfaces;
- comprehensive, step-by-step probing of the sub-systems and interfaces with a more meticulous scrutiny of the critical areas;

- identification and recording of the hazardous circumstances including causes, consequences and potential mitigation and control measures;
- expert driven ranking of the identified hazards employing an appropriate frequency/consequence matrix;
- maintenance, update and management of the records throughout the life of the product, process or undertaking.

The hazards identified through the empirical processes must be reviewed at appropriate stage(s) during the creative phase and recorded together with the other attributes alongside the newly identified items in a log. The empirical phase is sometimes employed as a completeness test or means of detailed probing of specific hazards and failures, subsequent to the creative identification phase. Whichever the temporal order, the empirical and creative phases must be applied in a consistent and complementary manner to re-enforce and increase confidence in the hazard portfolio.

The two-phase process enhances the integrity and coverage of the potential hazard space, increasing the effectiveness and confidence in the safety and security process. It has to borne in mind that the hazard identification exhibits an essentially non-linear gain and a creative identification of a single significant hazard may outweigh the contribution of a large number of less severe items. In this spirit, it is the quality and not the quantity of the identified hazards that is of the essence. The methodologies that generate an unrealistically large number of mostly trivial hazards are wasteful of resource, misleading and unproductive and should be avoided wherever possible. Furthermore, the subsequent analytical treatment of hazards as detailed in this chapter should be applied on a prioritised basis, beginning with the highest-ranking hazards.

### 3.1.2 Causal analysis

Upon systematic identification and ranking of hazards arising from a product, process, service, system or an undertaking, it is often constructive and sometimes necessary to further explore the logical relationship between the basic errors and failures that could potentially realise the hazards. The aim is to address each hazard at the root cause level with a view to preferably eliminate and where not feasible, reduce the frequency or likelihood of its realisation (occurrence).

#### 3.1.2.1 Process

The causal analysis is a mainly empirical process requiring domain knowledge of the product, process, service or undertaking. The techniques of Causal Analysis are generally applied recursively in a top-down mode to a given general state (hazard or threat) until all low level specific causes, errors and failures are arrived at. This deductive approach generally produces a number of intermediate states, each potentially caused by lower level causative factors. The general heuristic is to continue with the decomposition of each intermediate state until all fundamental causal factors such as basic component failures, unintended human errors or malicious acts are arrived at or it proves impracticable to acquire reliable data pertaining to lower level factors. The causal analysis techniques are predominately applied within reliability engineering and are generally supported by mathematical foundations and a suite of computer based tools.

### 3.1.2.2 Modelling

The causal analysis techniques generally employ graphical modelling which constitute a potent form for the capture and communication of the inter-relationship of the primary errors and failures leading to a hazard or vulnerability. Whilst predominately employed qualitatively, the causal models often lend themselves to quantification that ultimately generates a probability or frequency for the hazard or threat under analysis. The key issues to bear in mind during the causal modelling process are:

- correct logical relationships;
- decomposition commensurate with data availability;
- common cause failures;
- redundancy;
- inter-dependency of some errors and failures.

It is also important to ensure that different variables expressed in probabilities or frequencies are combined appropriately to generate consistent results for example, ensure that two frequencies are not multiplied to yield units in terms of per time squared! An illustrative causal model for a railway hazard is depicted in Figure 2.

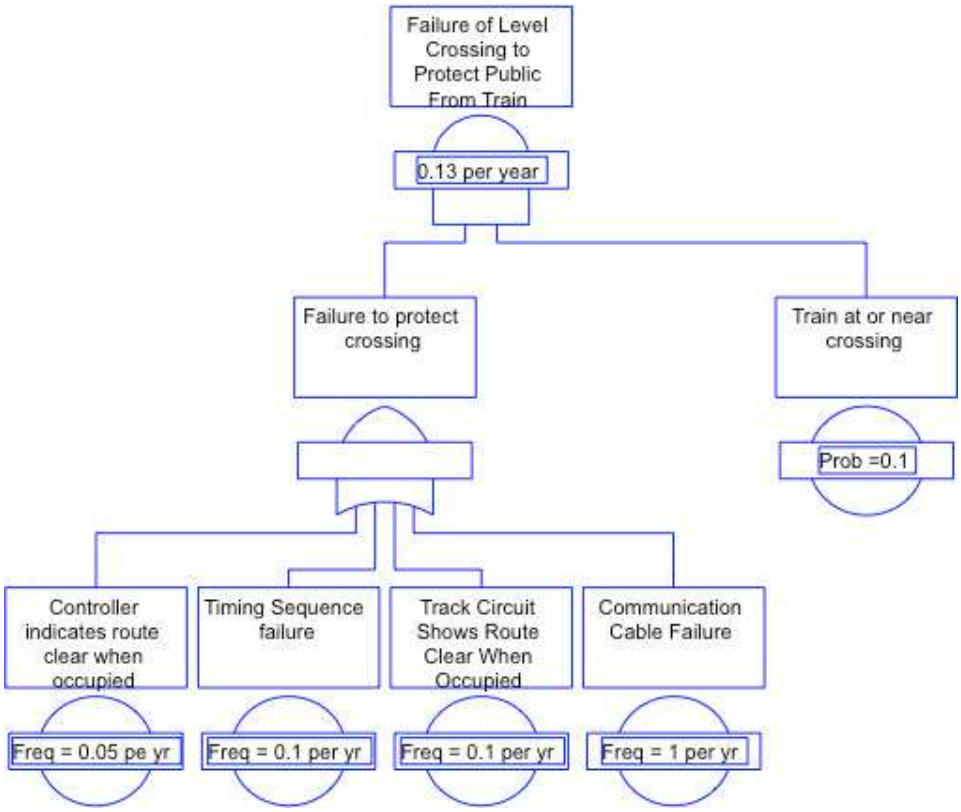



Fig. 2. Illustrative Causal Model for a railway hazard

#### 3.1.2.3 Quantification

The quantification of causal models entails an objective assessment of the potential frequency or likelihood for the causal factors. These are combined according to the rules of probability calculus and Boolean logic to generate a normalised or absolute measure for the realisation of the hazard or threat often referred to as the top-event in view of the top-down nature of causal modelling. The key issues to bear in mind during the provision and statistical processing of data for the quantification of causal models are:

- reliable and objective sources for the basic errors and failures;
- consistent application of compatible data types;
- appropriate pre-processing of the data e.g. mean over a number of years;
- uncertainty and non-linearity in the data;
- sensitivity and importance criteria for the errors and failures.

Where input data is specified with confidence intervals or a significant sample size is available, the use of statistical simulation techniques is essential in generating a probability or frequency forecast for the hazard or threat.

#### 3.1.2.4 Constraints

The causal modelling techniques are generally incapable of addressing temporal variations in data and only apply if frequencies and probabilistic errors and failures remain constant over time. Furthermore, causal models are often generated by individual domain experts and it is essential to subject these to peer review in order to enhance confidence in their integrity and correctness.

### 3.1.3 Consequence analysis

Whilst the causal analysis is aimed at establishing the factors leading to the realisation of a hazard or threat, consequence analysis is concerned about what may potentially follow the occurrence of a hazardous situation. This is the least understood and exercised mode of analysis to the extent that most established criteria for safety and security in vogue in industry are only concerned with the occurrence of a hazard and implicitly assume each occurrence necessarily equates directly with an undesirable catastrophic accident or loss. The notions of Wrong Side and Right Side Failure and their application as criteria for safety performance are indicative of this misunderstood discipline. In truth, the occurrence of a hazard may potentially lead to a broad range of consequences, some of which may probabilistically be undesirable events. The correspondence between the hazard and a catastrophic consequence/accident is seldom at parity i.e. it rarely follows that the existence of a hazard or threat can be assumed to correlate 100 per cent with the worst likely accident.

#### 3.1.3.1 The process

The consequence analysis is a largely probabilistic and potentially creative process requiring domain experience pertaining to the application of the product, process, system or undertaking. The techniques of Consequence Analysis are generally applied recursively in a bottom-up or forward inference mode to a given specific state (hazard or threat) until all potential general consequences (incidents and accidents) are arrived at. This inductive approach generally produces a number of intermediate states, each probabilistically leading

to a number of other likely intermediate states or consequences. The heuristic in this mode is to continue with induction at each intermediate state until all known barriers to the escalation of the hazard or threat are exhausted and all potential incidents, accidents or safe states are identified. The consequence analysis techniques are predominately applied within decision theory.

### 3.1.3.2 Modelling

The consequence analysis techniques generally employ graphical modelling which constitute a potent form for the capture and communication of the incidents, accidents and other benign states potentially arising from the realisation of a hazard or threat. Consequence models often in the form of trees lend themselves to quantification that ultimately generates a probability or frequency for each predicted incident and accident. The key issues to bear in mind during this modelling process are:

- clear understanding and definition of the hazardous or threat state to be analysed;
- existence of physical barriers (protection systems) to the escalation scenario ;
- existence of procedural barriers to the escalation scenario;
- existence of circumstantial barriers to the escalation scenario;
- the strength of each barrier's capability in preventing further escalation;
- the escalation path upon success or failure of the identified barriers;
- uncertainty and non-linearities in barrier strength;
- the inter-dependencies between various barriers to escalation scenario .

Where barriers to escalation are non-existent, it is possible to identify the need for protective measures in the course of consequence analysis i.e. the need for a non-existent detection system or procedure. Furthermore, if a hazardous situation is experienced and knowledge of its rate or likelihood of occurrence is at hand, consequence analysis would prove more beneficial than its causal counterpart in establishing the likely consequences and extent of potential losses. This might obviate the need for causal analysis in some circumstances.

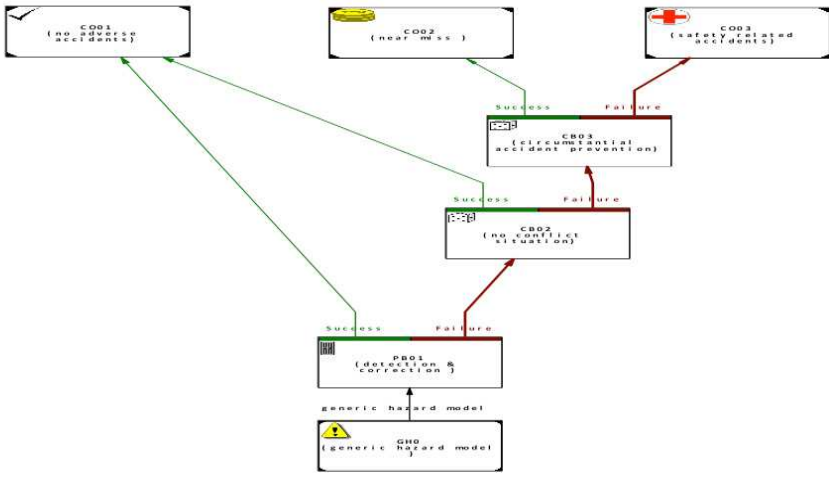



Fig. 3. Illustrative Consequence model for a railway hazard

It is prudent to explore the existence and effects of physical, procedural and circumstantial barriers to escalation scenarios associated with a hazard or threat in a systematic and ordered manner to ensure all potential safeguards are identified and incorporated in the consequence model. An illustrative consequence model for a railway hazard is depicted in Figure 3.

#### 3.1.3.3 Quantification

The quantification of consequence models entails an objective assessment of the potential strength (likelihood for success) for all identified physical, procedural and circumstantial barriers. These are either based on historical data, result of specific causal analysis or expert judgement where no objective data can be traced. The key issues to bear in mind during the provision and processing of data for the quantification of consequence models are:

- reliable and objective sources for the barrier strength (success probability);
- appropriate pre-processing of barrier data;
- uncertainty and non-linearity in the data ;
- dependency of barriers;
- sensitivity criteria for the barriers within a model.

Where input data is specified with confidence intervals, the use of statistical simulation techniques is essential in generating a probability or frequency forecast for the consequences.

#### 3.1.3.4 Constraints

The consequence modelling techniques are generally incapable of addressing interdependency, spatial and temporal variations in data and only apply if identified barriers to the escalation scenario retain a constant strength over time. Furthermore, in view of the probabilistic and creative nature, it is prudent to develop consequence models with the aid of a team comprising diverse domain experts as opposed to resorting to a single analyst.

### 3.1.4 Loss analysis

Loss comprises various degrees of harm to people, commercial/operational detriment to an enterprise or contamination/damage to the ecology of the environment or a combination thereof. It is associated with most undesirable consequences arising from the hazards of products, processes, systems and undertakings. Loss analysis constitutes the final stage of intrinsic hazard evaluation prior to adoption of reduction and containment strategies.

The statutory legal framework is mainly focused on prevention and regulation of harm to people and more recently, the environment. Commercial/operational losses on the other hand remain the prerogative of the business to avoid, transfer, mitigate, reduce or tolerate. In view of the diversity of needs and requirements, it is prudent to evaluate the losses associated with undesirable consequences in three distinct categories and aggregate these at a later stage. Loss analysis comprises the systematic investigation of the adverse outcome associated with all incidents and accidents identified through consequence analysis. The key processes in the evaluation of loss comprise:

- Safety Loss Estimation;
- Commercial/operational Loss Estimation;
- Environmental Loss Estimation.

Since the totality of loss is of the essence in the decision making process, upon evaluation, these need to be converted into a common currency and aggregated. The scale, scope and treatment of loss is context sensitive and in view of the inherent complexity, these are often treated subjectively.

#### 3.1.4.1 Safety loss evaluation or estimation

The evaluation or estimation of measures of harm to people arising from undesirable consequences such as collisions, derailments, fires and a whole host of man-made and natural disasters is dependent on a large number of context sensitive factors. The significance, causal relationships and dependencies between these factors are not adequately understood and most industries currently resort to published historical data for the estimation of safety losses. This is often in the form of statistical Means over a number of years and is fraught with a number principal difficulties namely:

- irrelevance of a historical mean to specific circumstances under study;
- distortion of means caused by rare catastrophic incidents and accidents;
- insufficient data regarding causal and contributory factors;
- variability due to introduction of different generations of technologies and infrastructures;
- secondary effects e.g. fires, derailments subsequent to a collision or exposure to harmful substances;
- poorly understood relationship between circumstances and loss severity;
- multiplicity of the types and classes of harm.

It is prudent therefore to establish an objective process for safety loss estimation that is capable of generating forecasts for the specific circumstances under consideration. The current practice severely undermines the effort spent in causal and consequence analyses of significant hazards in the industry and reduces the accuracy of the overall assessment process. It is also incompatible with the systematic framework depicted in this chapter. In the interim however, historical Means have to be appropriately scaled and processed to take account of specific circumstances predicted by consequence analysis, in order to give a semblance of reality and systematicity.

Safety loss should be measured in Minor Injuries, Major Injuries, Fatalities and Equivalent Fatalities. This is a process through which, various degrees of estimated harm to a given group of people exposed to the consequences of a hazard, is aggregated into an equivalent fatality figure for decision making purposes. The current convention is to aggregate fatality, serious injury and minor injuries in 1 : 0.1 : 0.005 ratio respectively in order to generate an estimate for safety loss in Equivalent Fatalities.

#### 3.1.4.2 Commercial/operational loss estimation

In addition to the potential safety implications, most incidents and accidents entail a measure of loss to the enterprises involved in terms of:

- disruptions to services causing delays;
- damage to movable assets;
- damage to infrastructure and equipment;
- loss of goods and material;

- loss of goodwill;
- loss of stake-holder/consumer trust and decline in custom;
- claims and potential legal fines;
- premium increases and other consequential losses.

An objective measure of these pertaining to the specific circumstances predicted by consequence analysis should be estimated, converted to a common currency (money) and aggregated to generate an overall figure for commercial/operational loss. Also note that whilst it is difficult to delegate safety and environmental duty of care, in the short term, their consequent losses including those due to commercial and operational loss can be largely transferred through contractual agreements and insurance.

#### 3.1.4.3 Environmental loss estimation

Apart from the commercial implications, release and dispersion of harmful substances in the environment as a result of incidents and accidents poses threats to health and safety as well as the eco-system. These may typically involve any combination of:

- fuels, oils, flammable substances;
- liquefied gases, explosives;
- caustic, corrosive and reactive chemicals;
- minerals and reactive material;
- radio-active materials;
- bio-toxins.

In addition to the immediate effects, further damage may be caused through dispersion into the atmosphere and contamination of land, water tables and rivers. The specific circumstances should be identified through consequence analysis. The environmental loss estimation may potentially involve an evaluation of the costs associated with:

- clean-up operations;
- containment strategies;
- emergency services;
- fines by Environment Agency, Rivers Authority etc.;
- Claims by other affected parties.

Systematic causal and consequence analysis may also reveal the need for further barriers to scenario escalation including protection systems, damage containment policies and emergency preparedness measures. It is prudent therefore to develop an objective process for the estimation of likely effects of incidents and accidents on the environment and convert and aggregate these in a common currency (money) to generate an overall figure for the environmental loss.

#### 3.1.4.4 Loss integration

The three broad categories of Safety, Commercial and Environmental loss may be realised as a result of incidents and accidents pertaining to hazards associated with the products, processes, systems and undertakings.

The evaluation of Health and Safety losses are required under the UK and most statutory frameworks in order to establish the tolerability and reduction of these to within reasonably

practicable levels. Further to legal compliance, the knowledge of the extent and scope of the safety, commercial and environmental losses provides the objective data for prudent business decision-making. However, it is useful for all three components to be converted and expressed in a common currency such as money for potential comparison and aggregation in order to provide a coherent view of the totality of potential loss associated with a hazardous situation. This ensures that safety and environmental issues become integral to often largely commercially driven decision making, enabling a realistic and balanced perspective on risk management within the enterprise.

The commercial and environmental losses or risks associated with each hazard are generally expressed in monetary terms. The safety loss or risk on the other hand is measured in terms of harm to people generally in the form of estimates or statistics pertaining to injuries and fatalities. A convention exists for normalising injuries and converting these to an Equivalent Fatalities (Lives). It is then possible to add injury forecast or statistics to fatality forecasts/statistics and produce a single estimate for safety risks in terms of Equivalent Lives. For aggregation with other mainly monetary losses, safety loss forecasts can further be converted into their equivalent monetary value employing the concept of Value of Preventing a Fatality (VoPF or VPF). This mainly statistical concept is sometimes referred to as Value of Preventing a Statistical Fatality (RSSB, 2006) and is purely employed to support safety related decision making and should not be misinterpreted as putting monetary value of lives of individuals. It is customary to employ the product of equivalent fatalities estimated for a product, process, system or undertaking by the industry benchmark for VoPF to develop an objective measure of total safety losses as a basis for further safety investment and prevention of such losses. This is intended to transform safety based investment and decision making from a fundamentally moral imperative to a rational process that can be contrasted and enforced globally with the key variant being the VoPF for the given circumstances under consideration. The adoption of a systematic risk framework and setting of a global value for VoPF to underpin enforcement of safety considerations in major undertakings is an imperative for transparency, fairness and demonstration of duty of care as witnessed in the controversy surrounding the large scale North American oil exploration disasters (BP, 2010).

### 3.1.5 Options analysis

The hazard identification process reveals a portfolio of circumstances that are subsequently prioritised and analysed through causal, consequence and loss analyses. Depending on the consequent losses, the hazards may subsequently require risk elimination, mitigation, transfer, control or an appropriate combination thereof. The identification, ranking, evaluation and management of viable pro-active hazard rate reduction (causal level) and largely re-active containment (consequence level) strategies constitute option analysis.

The identification and ranking of options is carried out within a process analogous to that defined for the hazards although, causal and consequence analyses of a hazard also serve to characterise appropriate rate reduction and containment strategies.

A number of options should generally be identified and recorded for each hazard or groups of synergistic hazards, taking into account established and emerging technologies. The options portfolio comprises those that precede the occurrence of a hazard (RO type) and

those that are effective post hazardous event (CO type). The options that precede the hazard horizon are primarily aimed at elimination or rate reduction hence labelled as Reduction Options (RO). The RO type measures are generally aimed at the prevention or retardation of the causal factors and are usually evaluated with the aid of causal analysis tools.

The options that are effective post occurrence of a hazard are mainly aimed at loss Containment (CO) and constitute further barriers to the escalation scenario. The CO type measures are usually identified or assessed with the aid of consequence analysis. Irrespective of the type mix, the options portfolio must be reviewed at reasonable intervals in order to ensure compliance with the ALARP principle in the context of management of safety risks in the UK or other statutory criteria.

A sensitivity parameter may be derived for the RO and CO type options through the causal and consequence models in order to ascertain the most effective measures for risk reduction and containment.

For each option, the annualised or the Net Present Value of the associated costs over the effective life must be evaluated and assessed as appropriate and recorded for comparison against potential benefits derived during through impact analysis.

### 3.1.6 Impact analysis

Upon identification and recording, it is essential to estimate the likely effects and potential benefits of each option on the consequent safety, commercial and environmental losses in order to establish the objective and systematic criteria for selection and implementation. This is a requirement of the statutory legal framework in the UK to ensure and demonstrate that the safety risks arising from a product, process, system or an undertaking are reduced to As Low As Reasonably Practicable (ALARP) levels.

Impact analysis comprises a systematic analysis of the beneficial and any detrimental effects of implementation of an option with a view to eliminate, reduce, mitigate, transfer or control the risks rising from a given hazard.

#### 3.1.6.1 RO type impact

The pro-active elimination or Reduction (RO) options are generally the preferred type and require treatment within the context of causal analysis. This generally involves incorporation of the option within the causal model or an assessment of its likely effect on the causal factors and appropriate adjustment of the rates or probabilities for each affected error or failure. The consequent safety, commercial and environmental Losses are subsequently re-evaluated through consequence and loss analysis. The Equivalent Lives differential thus evaluated pre and post implementation of an option should be recorded together with corresponding commercial and environmental loss differentials. These collectively constitute the Impact Parameters associated with the option and are employed in conjunction with the cost estimate in order to derive the safety and business criteria for the implementation of the option.

#### 3.1.6.2 CO type impact

The mainly re-active Containment (CO) type options comprise detection and protection systems and procedural barriers to further escalation of a hazard. This class of options are

generally effective in the post hazard horizon in that they will not affect the realisation of a hazardous state but assist with reducing the likelihood of a hazard transforming into accidents or the consequent accidents causing as much loss. The CO type measures should be evaluated through the consequence model of a hazard with their probability of success judiciously set to reflect their potential effectiveness on demand. In view of the time and resource implications, the CO type options should preferably be incorporated into a consequence model during the knowledge elicitation and capture of consequence scenarios. In this case, their effectiveness should be defaulted to zero until impact analysis provides the necessary criteria for implementation or dismissal.

In a similar process to that for RO type options, the evaluation of CO type measures entails the derivation of resultant safety, commercial and environmental Losses/risks subsequent to the adjustment of the effectiveness parameter. The Equivalent Lives differential evaluated pre and post implementation of the CO option should be recorded together with corresponding commercial and environmental loss differentials ideally computed in net present value terms if the effects are considered over a period of time. These Impact Parameters are employed in conjunction with the cost estimate arrived at during options analysis, ideally computed in net present value form, in order to derive the safety and business criteria for the implementation of the option.

### 3.1.7 Demonstration of ALARP and compliance

The demonstration of compliance with the regulatory requirements and the ALARP principle in the UK (HMSO, 2001) necessitates an assessment of individual risks arising from the undertaking, product, process or system for the members of the affected groups (Employees, Customers and the General Public). Individual risk represents an average across a group and its assessment is contingent upon the knowledge of the totality of risk and the size of the exposed group within the population. It is also customary to consider the most at risk amongst the groups affected since the exposure patterns will differ even for the members of the same group. However such detailed differentiation is only justified when patterns of risk exposure in a given population or group are vastly different to the average and supporting data justifies such elaborate considerations.

#### 3.1.7.1 Demonstration of ALARP

Within the context of UK regulatory legal framework, a duty is imposed on those who create a specific risk to health, safety and welfare of their employees, customers and the general public to ensure and demonstrate that these are reduced to As Low As Reasonably Practicable (ALARP) levels. The criteria for tolerability of risks has been published by UK's Health and Safety Executive (HSE), in terms of numerical targets for the individual risk of fatality for a specific group of people, exposed to the risks arising from a product, process, system or an undertaking. The HSE criteria effectively define an upper quantitative limit for individual risk of fatality beyond which, risks should not be tolerated, save in extraordinary circumstances. Risks falling below the upper limit of tolerability are expected to be subject to mitigation on a cost benefit basis, unless these are around two orders of magnitude smaller than the upper limit. It is important to note that the tolerability concepts apply at a holistic level i.e. to the totality of risks and not generally at the individual hazard level.

The demonstration of compliance with the legal duty of care and ALARP principle entails the following stages:

- identification of the hazards and the exposed groups potentially associated with the application of a product, process, system or an undertaking and treatment of the hazard portfolio under the qualitative and/or quantitative framework as appropriate with a view to assess the likely safety losses/risks associated with each hazard;
- development of a total risk profile for the product, process or undertaking in safety terms (the evaluation of the commercial/operational and environmental risk categories should also prove valuable);
- identification of elimination, rate Reduction (RO) or Containment (CO) option(s) for each hazard;
- determination of the net present value cost and impact of option(s) on the safety loss associated with the corresponding hazards;
- determination of cost effectiveness for the identified options and derivation of Cost Safety Benefit (equivalent cost of saving a fatality through application) for each option;
- Implementation of all options for which Cost Safety Benefit is smaller or equal to the Value of Preventing a Fatality (VoPF) or other industry criteria (Hessami, 1999). The concept of gross disproportion should be applied to disparity between the Cost Safety Benefit of an option and the VoPF convention, depending on the magnitude of the total risk;
- recording of the data, assumptions, calculations and consequent decisions.

Whilst this process accords with the guidance given for the qualitative assessment of less significant risks, it is insufficient within the context of major risks that may violate the tolerability criteria. However, it ensures that all risk elimination, mitigation and control options are assessed and implemented, thus reducing the totality of risks to As Low As Reasonably Practicable level, but cannot determine tolerability against the published benchmarks. Furthermore, for new products, systems and processes, by focusing on individual hazards, the approach only ensures compliance with ALARP for the adopted design or approach. It would not guarantee the optimal low risk solution that might involve a different hazard portfolio. Optimisation of risks arising from products, processes, systems and undertakings is beyond the scope of the current discussion.

The determination of the tolerability of risks and the significance of gross disproportion as a criterion for the implementation or dismissal of the options requires a comparison of the totality of risks against apportioned industry benchmarks. This is achieved through the complementary demonstration of compliance stage.

#### 3.1.7.2 Demonstration of compliance

Whilst the achievement and demonstration of lowest practicable levels of risk is broadly sufficient for the demonstration of legal duty of care, it is not suitable for determination of the tolerability, against industry performance benchmarks. Furthermore, in dealing with major risks within a quantitative framework, implementation of risk reduction and containment options cannot be carried out in isolation from the knowledge of the position of overall risk within the tolerability scale.

The industry safety performance benchmarks in the UK are generally derived from the Health and Safety Executive's guidance on industrial risks and criterion for tolerability. However, the benchmarks represent an annual average for the individual risk, influenced by a vast and diverse range of products, processes and undertakings. These benchmarks generally lie within the middle of the tolerability scale for each affected group, which is bounded by upper and lower numerical limits.

The comparison of the aggregated risks of a product, process or an undertaking with the published benchmarks requires an assessment of the contribution of the particular item under consideration to the industry's annual safety performance. This is known as apportionment, which in the absence of a systematic dynamic model for the whole of an industry is an un-productive and unsystematic exercise. In the absence of such a model, a simple rational argument and calculation for apportionment is preferable to the often wasteful and expensive efforts in manipulating historical data.

The demonstration of compliance with the industry safety principles and performance benchmarks entails the following stages:

- A review and justification of all identified hazards and mitigation options against industry or regulatory safety principles;
- aggregation of the safety loss of the hazards in the portfolio generating a total risk estimate for the product, process or the undertaking for each affected group;
- estimation of the size of population exposed to the risks in each group;
- calculation of the average risk per person in each group;
- apportionment of the industry benchmarks to the specific contribution of the product, process or undertaking;
- comparison and determination of tolerability against apportioned benchmarks;
- if the risk is intolerable, i.e. it exceeds the upper level of tolerability, it shall be reduced to within tolerable levels or the product, process or the undertaking abandoned, save in extraordinary circumstances;
- if the risks are tolerable, follow a process as for demonstration of ALARP bearing the following in mind:
  - if the computed individual risk is close to the upper limit of tolerability, a gross disproportion between the Cost Safety Benefit and VoPF should be the criterion for implementation of RO and CO options.
  - if the computed individual risk is close to the lower limit of tolerability, the parity between the Cost Safety Benefit and VoPF should be the criterion for implementation of RO and CO options.

In view of the current uncertainties and inaccuracies inherent in the apportionment process, the demonstration of compliance with the industry benchmarks should be treated as a coarse and relative indicator of safety performance of products, processes and undertakings. It is imprudent therefore to treat the individual risk calculations and the apportioned benchmarks as the sole dependable absolutes for decision-making.

### 3.2 Risk management system – Principles

Compliance with the requirements cited above requires a systematic scrutiny of defect/error-failure-accident scenarios to ensure a comprehensive risk perspective. In

reality, adopting a hazard and threat based approach to risk assessment and management generates a more systematic framework for coping with varieties of risks. A defect-error-failure sequence is proposed to address the processes leading to the realisation of a hazardous state or event in a product, process or system. Consideration of the post hazard horizon in this approach involves identifying the potential escalation scenarios, the defences against accidents, the range of accidents that arise due to the failure of defences and optimal response and recovery regimes for each major accident scenario. In a similar manner to the assessment regime, the systematic framework for risk management comprises the following seven principles:

i. Prediction and Proactivity;
ii. Prevention;
iii. Containment & Protection;
iv. Preparedness & Response;
v. Recovery & Restoration;
vi. Organisation & Learning;
vii. Continual Enhancement.

These principles collectively address the total risk landscape and are inter-related in a systemic fashion. They also relate to the framework for risk assessment in a consistent and demonstrable way. The principles are detailed below.

#### 3.2.1 I – Prediction and proactivity principle

The primary principle in systematic assurance is that of "prediction" which involves analysis and identification of credible system modes and potential loss/hazardous states, anticipation of escalation scenarios, evaluation and assessment of the baseline risks and taking hard and soft risk control measures in advance of foreseeable accidents. This by necessity involves developing and implementing methods and procedures to assess the risks and establish the baseline performance in order to support the case for further risk reduction, control or mitigation as appropriate.

The principle is the focal point for the identification (prediction) of foreseeable activities, modes and states within a system that adversely affect performance (safety, operational, environmental, RAM etc.) comprising Normal, Degraded, Failure and Emergencies and the triggers and transitions for these.

The administrative, strategic and implementation facets of performance are addressed through "proactivity" comprising policy, planning, resourcing and determination of strategy and plan for compliance with existing, emerging and modified directives, regulations, rules and mandatory standards. Proactivity also implies setting the ground rules and the scene for Prevention, Protection, Response and Recovery policies (see other principles).

Establishing communications channels between internal and external stakeholders including the production of a Safety Case for the organisation/undertaking, a Safety Management Manual, a Document Management System and a Configuration Management and Change Control System also fall within the scope of Proactivity.

### 3.2.2 II – Prevention principle

Once the baseline performance is established through "prediction" and the need for risk reduction is identified, the "prevention" strategy provides the most logical and prudent approach to the realisation of this objective. Prevention principle addresses the analysis of the known and new hazards/threats, understanding of their causation chain and identification of the measures capable of eliminating or reducing the likelihood of occurrence of the threats/hazardous states.

Prevention strategies are best attempts at reducing defects, errors and failures and comprise a broad range of technical, procedural and human competence related measures. This is the cornerstone of most industries' traditional approach to ensuring safe/secure states through design and implementation of fail safe systems, inspections, preventative maintenance, selection, training and briefing of staff. However, whilst prudent, these measures fail to completely eliminate or control the threats/hazardous states thus assurance of desirable performance of the overall system cannot be relied upon the success of preventative strategies alone.

The "prevention" focus ensures all causations and escalation routes to the threats/hazardous states are identified, analysed and all credible and reasonably practicable elimination and control measures are evaluated and implemented. This includes scheduled and preventive maintenance activities aimed at maintaining the functionality and integrity of the system.

### 3.2.3 III – Containment & protection principle

The thrust of the classical approach to performance assurance of systems, services and operations is embodied in the designs, architectures, rules, processes, systems and behaviours that are mainly based on the Prevention philosophy as cited before.

Whilst allocating resources and focusing attention on *prevention* is rational and prudent, it should not be at the expense of the mitigating risks, once undesirable hazardous events occur or threats are realised. The aim here is to determine the escalation mechanisms/scenarios for hazardous conditions and establish strategies, responsibilities and timely responsive action aimed at containing the energy or potential of hazardous states/threats in such a manner that they would not escalate into accidents potentially causing commercial, environmental and human harm/loss.

The preference here is to set up effective barriers to escalation and where possible, turn loss prone or hazardous occurrences into incidents or lower severity accidents. The second aspect to this is to attempt to "Protect" the people/property at risk against potential injuries, fatalities and collateral damage should accidents occur or attempt to reduce the severity of such harm/damage.

The Containment and Protection Principle is developed and proposed in recognition of the fact that in spite of major efforts by duty holders, hazardous states do occur and threats do materialise in any system or environment often driven by complexity and change or adoption of unproven yet promising technologies. It is prudent therefore to have strategies, plans and measures in place to reduce the harm which would otherwise be caused by the escalation of these states if not controlled in a timely and effective manner.

The Protection focus ensures that the escalation paths for credible loss prone/hazardous states are recognised and reasonably practicable measures (barriers) are identified, assessed and adopted/strengthened to detect and rectify the hazard/threat escalation and where not possible mitigate the consequences.

### 3.2.4 IV – Preparedness and response principle

The essence of risk management lies in the success of the Proactivity, Prevention and the Protection strategies and prudent risk control initiatives. However, in view of the complexities inherent in the many industrial, infrastructure and service sector operations, accidents do occur from time to time. In the same spirit, a high degree of anticipation and preparedness for responding to accidents, emergencies and degraded modes of operation is an integral facet of ensuring the impact is kept to a minimum.

The *preparedness* is an aspect of organisational and resource planning and provision which entails anticipating, planning, resourcing, training and clarifying roles, responsibilities, communications, command structure and resources to address critical classes of degraded, failure and emergency states occurring within the operational environment. This by necessity requires a degree of learning from past experience as well as anticipating new scenarios when changes are enforced to the organisation, composition, structure or the operation of the systems being managed.

The *response* dimension of the principle is mainly concerned with the implementation of the Preparedness plans comprising:

- mobilising resources for presence on the scene and in support roles;
- protecting the site;
- evacuating the affected parties and the public;
- determining a command structure to manage each event;
- informing relevant civil authorities and emergency services with a view to protect and rescue those exposed or involved in the circumstances and minimise the degree of harm which would otherwise be sustained;
- minimising overall harm and loss arising from an accident.

The *preparedness* and *response* principle also addresses contingency scenarios i.e. new/unexpected degraded, failure and emergency aspects and circumstances for which, a general class of reaction is required as a safety net against all unforeseen cases. The *preparedness* and *response* focus ensures optimal reaction to accidents, catastrophes and security related losses is recognised and attained with a view to minimise safety and property losses in such circumstances.

### 3.2.5 V – Recovery & restoration principle

The timely and appropriate response to incidents and accidents ensure that people and collateral exposed to threats, hazardous states or accidents receive optimal help and support with a view to minimise any harm/damage which would otherwise be incurred in the circumstances. However, depending on the severity and nature of the degraded, failure or emergency state, a degree of anticipation, advance planning and resourcing is required to initiate timely and efficient *recovery* activities on the affected system or infrastructure.

Recovery after incidents and accidents essentially begins after *response* process has resulted in securing the safety of the affected or exposed people and is mainly concerned with the processes and resources to repair the damage incurred in a safe, timely and efficient manner working towards the *restoration* of the system to normal state/service. It may also arise from disturbances to the system including preventive or reactive maintenance when the system is being brought back to normal operational state. Depending on the nature of the degraded, failure or emergency, the *recovery* activities may additionally impose various risk control restrictions on the functionality, infrastructure or the operation of the system.

The *restoration* addresses the rules, processes, roles, tests, competencies and authorities required to ensure the state of the infrastructure or operations after the *recovery* activities are technically sound, efficient, affordable and acceptably safe for return to restricted or normal service. In this spirit, *recovery* and *restoration* are assurance related activities. Restoration may be achieved in a number of phases culminating in the full resumption of the normal operational state.

The *recovery* and *restoration* focus ensures the repairs to the infrastructure and the service/production system post disturbances (including maintenance) and accidents is carried out in a safe and efficient manner and the subsequent deployment is subject to a systematic test, verification and validation process.

### 3.2.6 VI – Organisation & learning principle

The achievement, maintenance and improvement of the overall performance of any system or operation is contingent on timely appropriate actions assured through a learned and competent human organisation.

The Organisation Principle addresses the entire spectrum of human resource issues pertinent to the maintenance and improvement of performance. These include recruitment, induction, deployment, training, development briefing and communication of critical issues, qualifications, physical fitness, certification and regular verification and validation of the capabilities and competence.

Traditionally, assurance is treated as a specialist discipline and relegated to a particular group of staff solely concerned with this objective. However, whilst performance assurance like other disciplines has its specialist niches, its recognition, understanding of the underlying concepts, care for other people's health, safety and welfare constitute a broad suite of beliefs, values and practices referred to as organisational culture. The recognition, promotion and nurturing of this culture is a crucial factor in the success of policies and initiatives within an organisation. Assurance culture promotes the notion that apart from specialist activities, knowledge, practices, beliefs and values in accident prevention should be common to all who have a role in the provision of service or systems with a potential to cause harm to the customers, employees and the general public or damage to the environment and property.

The organisation does not necessarily imply a dedicated arrangement for risk management, fundamentally separate from other functions of the business or service organisation, infrastructure management or other stakeholders. Apart from specialist activities, a supportive and pervasive assurance culture must be developed and promoted throughout

the enterprise including education, briefing and establishment of a confidential channel for communication of observations, suggestions and feedback on all performance related matters. In this spirit, the principle underpins all other aspects of the framework since it provides the human motive force for realisation of all other principles inherent in assurance management.

The other facet of the organisation principle is the ability to learn and capitalise on the new and emerging knowledge for improving performance. A key instrument supporting the learning process is development, implementation and maintenance of a corporate memory to underpin the recording, retrieval and processing of relevant knowledge and resultant learning. The corporate repository of performance information must include an up-to-date directory of infrastructure, systems and operational threats/hazards that needs to be initiated at system level whilst being updated for local conditions. This repository must be made accessible to all stakeholders to inform them about all pertinent issues which may relate to their roles, tasks and undertakings within the system.

The repository of performance information should additionally include records of reported failures, threats, incidents and accidents and any analysis establishing causation, escalation mechanisms and the degree of harm or damage caused. It is crucial that these are captured, shared openly and employed actively to enhance systems and processes with a view to prevent future occurrences (prevention principle). This is a costly but essential aspect of learning from what in principle amounts to the failures of the Management System.

Finally, the organisation principle must cater for the relationships, reporting structure, licensing and responsibilities of various organisations involved in the design, installation, operation, maintenance and disposal of the infrastructure, service delivery, production system and its constituents.

The focus on organisation and learning ensures that competent people are recruited, trained and tasked with assurance related activities and lessons are learnt from faults, failures, incidents and accidents with a view to eliminate or minimise future occurrences.

### 3.2.7 VII – Continual enhancement principle

The principles and their inherent activities cited earlier can underpin achieving and sustaining a desirable performance in the context of a product, process, service, system or undertaking. However, improving quality of life, advancing social values and consequent emerging legislation, rules and standards tend to demand more stringent targets, more responsive behaviours and improving overall performance. The other key driver is the rising consciousness in the society about duty of care and negligence by people and organisations delivering services and products and the consequent criminal and civil claims in the event of accidents causing harm to victims or financial loss to the stakeholders.

The inherent complexities of the infrastructure, production systems and operations in industrial and service sectors as well as the increasing demand for incorporation of novel technologies pose a challenge to the maintenance of performance levels during the transition. A rational, systematic and scientific approach to the traditionally empirical

treatment of assurance matters in the industry is called for. Identification of key performance indicators, measurement and proactive control of risks are key instruments in the new approach.

The *continual enhancement* of various facets of performance necessitates an objective appreciation of the existing drivers, actors, faults, failures, hazards, threats, targets and existing performance levels before reasonably practicable options are identified, assessed and adopted for improvement. To this end, a comprehensive approach to identification, monitoring and measurement of precursors to accidents, agreement on relevant performance criteria and normalising factors, audit of safety and security processes and culture, review of targets and making a case for performance improvements constitute the essence of this principle.

The enhancement of performance may arise from the introduction of novel feature/functionalities, identification and strengthening of the barriers to causation or escalation of the hazardous states or complete elimination of hazards through adoption of new materials and technologies. The extent and scope of the performance improvements may be driven by revised targets, new standards or emerging lower cost technologies making risk reduction reasonable when contrasted against the likely gains.

The corporate repository of performance information cited under the *organisation* principle should also be actively reviewed for detecting trends in the underlying causes and breaches, precursors to accidents and near hits (strangely referred to as near misses). This information should be communicated with all stakeholders and employed as a potent tool to systematically eliminate the unacceptable levels of faults, failures and errors arising from human or automation sources, thus preventing accidents.

The focus on *continual enhancement* ensures attainment of tolerable levels of overall performance is treated as a dynamic and evolving objective subject to a systematic and on-going measurement and assessment regime to support credible understanding of the performance thus underpin the need and quest for sustaining good performance and enhancement.

### 3.2.8 Risk management framework

The seven principles inherent in the performance assurance of products, processes, services, systems and organisations fall into three broad categories;

The first principle, *proactivity*, is mainly concerned with establishing an environment and a baseline for the product, process, service, system or organisation in terms of its desirable properties and performance. It represents an antithesis to reactivity in facing the potential of accidents. In this spirit, *proactivity* is fundamental to the achievement and improvement of performance since it emphasises that plans and resources must be devised, secured and applied in advance of incidents, threats and accidents to enable the duty holders to eliminate, control or mitigate the risks.

The second group comprising *prevention*, *protection*, *response* and *recovery* are mainly associated with causation and escalation of accidents and the optimal preparedness in responding to these and emergencies with a view to minimise losses.

The third and final group of two principles relate to the significant role that the human organisation, communications, responsibilities, competencies, certification, regulation and corporate memory/learning play in the attainment and improvement of overall performance. This includes a drive for continual enhancement based on an audit, measurement and feedback loop to ensure a set of common indicators are continually monitored to empower the duty holders to take effective remedial and improvement actions as appropriate.

The seven fundamental principles collectively constitute a systematic and systemic framework for assurance of overall performance in the face of threats and risks. These are outlined in Table 1.

| *Principle* | *Scope & Intent* |
|---|---|
| I. Prediction & Proactivity | Setting Policy and Strategy, identifying all stakeholders and interfaces, Hazard/Threat Identification, planning, resourcing and data collection. Modelling, assessing baseline risks, identifying key performance indicators and implementing policy. Developing Safety, Security & Sustainability Cases and relevant Management Manuals |
| II. Prevention | All measures, processes, activities and actions including maintenance aimed at eliminating or reducing the likelihood/frequency of threats/hazardous states with a potential to cause harm and loss |
| III. Containment & Protection | All measures, processes, activities and actions aimed at reducing the likelihood/frequency or severity of potential accidents arising from the hazardous states or security breaches |
| IV. Preparedness & Response | All plans, measures, processes, activities and resources relevant to managing degraded and failure modes and emergencies, investigation of the causes, collection, maintenance & sharing of records |
| V. Recovery & Restoration | All plans, measures, processes, activities and resources relevant to recovery from planned and unplanned disturbances, degraded and failure modes and emergencies towards full resumption of production/service including the criteria and organisation for authorising the system back into service post disruptions and emergencies |
| VI. Organisation & Learning | Structuring, communications, training, certification, competencies, roles & responsibilities and validation for human organisation as well as ensuring lessons are learnt from incidents and accidents and key points recorded, shared and implemented |
| VII. Continual Enhancement | All processes associated with setting and reviewing targets, measuring/assessing, processing, auditing, reviewing, monitoring, regulating and sustaining/improving performance including decision aids and criteria |

Table 1 The Systemic Assurance Framework of seven Principles

The framework depicted in Figure 4 represents a constellation of complementary and inter-related principles which when applied collectively, can systematically underpin the attainment, maintenance (principles I-VI) and improvement (principle VII) of overall performance. A framework founded on systemic principles is more fundamentally credible, stable and universally applicable than specific context related suite of actions, processes or methodologies.

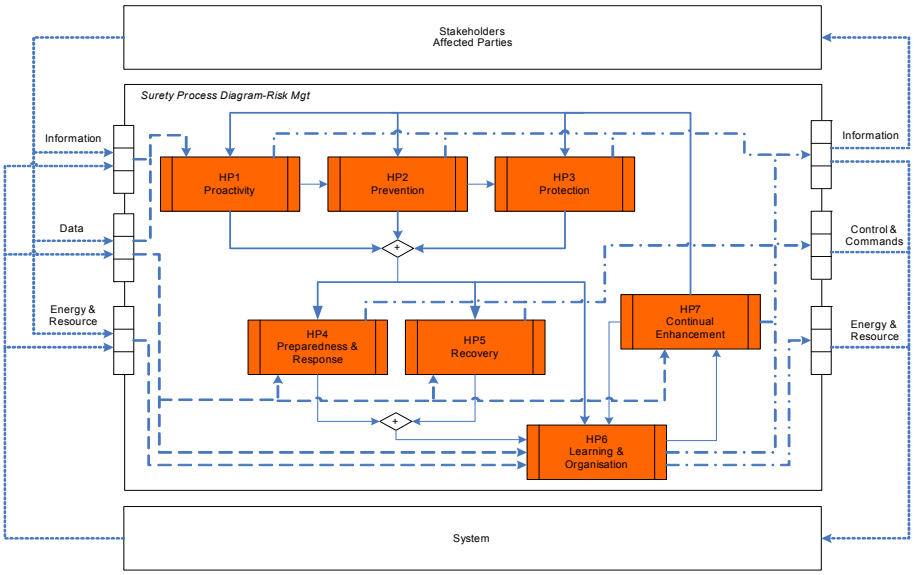



Fig. 4. The Systematic Framework for Risk Management, its Interfaces and Interactions

### 3.2.9 Systemic characteristics of the management framework

Whilst holistic and complete, the proposed framework for risk management possesses essential properties such as simplicity, rationality and a level of abstraction that lends it adaptable to any context, scale and organisation. These are crucial to the stakeholders understanding, adapting and applying it to optimal effect.

The framework transforms the traditional focus on accidents and loss to understanding, control and management of threats and hazards. This fundamental shift of emphasis yields a more profound knowledge on the root causes of faults, errors and failures thus resulting in a more effective management of business and operational risks.

The framework sets out all the building blocks for systematic risk management starting with establishing the environment and baseline performance (principle I) leading to four focal points (principles II-V) for actualising plans and policy. A major emphasis is also placed on the organisational facets from performance focused structure, roles, responsibilities, accountabilities, competencies and communications to the more subtle cultural aspects (principle VI). Finally an active learning ethos and actualisation of learning in improvement of overall performance is emphasised in principles VI & VII. The

intangible human dimension related to buy-in, motivation, participation, conflict resolution and taking people and property into account in everything we do is often ignored or not given sufficient prominence in existing management frameworks and standards.

The principles are not things to do per se. They constitute a complete strategic perspective and roadmap providing the essential focal points for the requisite activities and processes inherent in the systematic assurance of performance in products, processes, services, systems and undertakings. In this spirit, each principle also constitutes a focal point for measurement, benchmarking and determination of the status, success or shortcomings of the specific aspects of the Risk Management System.

The principles within the framework are goal-oriented and apart from guidance on the purpose and nature of essential activities, are designed to allow specific stakeholders to adapt these to their roles and circumstances and innovate to improve performance. This is particularly relevant to the historically diverse nature of the international trade with different cultural and structural underpinnings to the participants and stakeholders.

The four key focal points (principles II-V) on the actualisation of the plans and policies empower duty holders to collaboratively contribute to the overall performance of their operations. These principles would naturally involve a different set of activities for an each stakeholder organisation but none-the-less remain equally applicable at the framework level hence the need for scalability and adaptability.

The proposed principles are valid at any stage of the life-cycle (ISO/IEC, 2002) therefore, they are equally applicable to any group or organisation involved in the provision of service, products or management of infrastructure, production and operations. These can provide proactive indicators to assist the duty holders with their tasks as well as those responsible for the supervision and regulation of the relevant industry.

It would therefore be feasible to audit, assess and score an organisation's processes, capabilities and maturity in Proactivity, Prevention, Protection, Response, Recovery, Organisation and Continual Enhancement as appropriate to the nature of the undertaking. These scores and proactive criteria when benchmarked, will signify the status, strengths and shortcomings of an organisation in their systemic approach to the management of risks (Hunter & Hessami, 2002).

Apart from audit, assessment and scoring of the individual principles, it is also possible to generate an overall index of merit for the performance of the whole framework, thus giving a holistic indication for the capabilities and maturity for an organisation in its risk management endeavours. This provides an objective and constructive framework for intra-industry benchmarking, comparisons and enhancements.

The proposed framework is founded on seven systemic principles that can underpin performance assurance when applied in aggregate. In this spirit, the architecture of the proposed framework is entirely scalable and can be adopted to manage risks at the level of a product, process, team, project, department, organisation, an alliance of organisations and

an industry as a whole or any larger aggregate of these constituent entities. At every level of the application, the essential invariant aspects of the framework i.e. the seven inter-related principles, require mapping and adaptation to the nature, scale, context, tasks and the application.

## 4. The way ahead

Our systems approach to the holistic treatment of risks recognises the need for examination, understanding, characterisation and assessment of principal threats and hazards followed by a requisite suite of principles as a focal point for monitoring, supervision and management of resources to sustain performance. This has resulted in two systemic frameworks, one focused on identification, evaluation and assessment of risks and the other comprising seven principles on the performance assurance and management of risks.

The seven principles underpinning the assessment of risks cited above constitute a comprehensive and disciplined framework capable of rendering a thorough understanding of the key threats, hazards and the magnitude of potential risks associated with these in a given context. However, these are not adequate to maintain effective control and assurance.

The approach to the holistic management of risks is best served through a systemic framework comprising principles that hold true in different sectors, levels of hierarchy, contexts and circumstances. The principled approach generates consistency, integrity and a familiar harmonised process to underpin assurance activities. However, the principles in a framework only constitute focal points for allocation of resource and energy and require mapping to the specific characteristics and demands of an environment, sector, system or undertaking.

A framework of seven principles developed and proposed for risk management addresses the risk management requirements comprehensively and holistically. The framework is equally applicable to security issues pertinent to the malicious intents and can provide one consistent and systemic environment for successful management of safety, security and potentially sustainability risks pertinent to products, processes, services, systems and undertakings in railways.

Because of its principled constitution, the two frameworks are scalable and can be applied at any level and within any industrial, infrastructure and service sector context. The risk management framework has been adopted by the EU - Project "Safety and Reliability of Industrial Products, Systems and Structures" (SAFERELNET), funded by the European Commission under the "Competitive Sustainable Growth" programme (SafeRelNet, 2006). This has recently been published in an accompanying book to the work of the SafeRelNet network (Guedes Soares, 2010).

## 5. References

A Look at China's High-Speed Rail Investments, http://www.solarfeeds.com/, Tuesday, 04 May 2010 The Green Leap Forward

Chaudhury, Abijit. Jean-Pierre Kuilboer. (2002). *e-Business and e-Commerce Infrastructure*. McGraw-Hill, ISBN 0-07-247875-6.

Chrissis M.B., Konrad, M., Shrun S. (2007) *CMMI Second Edition, Guideline for Process Integration and Product Improvement*, ISBN 0321279670.

*Engineering Safety Management* Issue 3 (Yellow Book III), Volumes 1 & 2, Fundamentals and Guidance, Railtrack PLC UK, January 2000, ISBN 0 9537595 0 4.

European Standard EN50129 *Railway Applications – Communications, Signalling and Processing Systems – Safety Related Electronic Systems for Signalling*, CENELEC - February 2003.

Hessami, A. (1999) *Risk Management a Systems Paradigm*, Systems Engineering-The Journal of the International Council on Systems Engineering, Volume 2 Number 3, pp156-167.

Hessami, A. (1999). *Safety Assurance, A Systems Paradigm*, Hazard Prevention- Journal of System Safety Society, Volume 35 No. 3, pp8:13.

Hessami, A. (1999). *Risk, A Missed Opportunity*, Risk and Continuity Journal, pp2:17-26.

Hunter, A. and Hessami, A.G. (2002). *Formalization of Weighted Factors Analysis*, Knowledge-Based Systems.

Hessami, A.G. (May 2004) *A Systems Framework for Safety & Security - The Holistic Paradigm*, Systems Engineering Journal USA Volume 7, Issue2.
http://www.demos.co.uk/

ISO/IEC15288 (October 2002), *System Life Cycle Processes* - ISO/IEC.

Miller, R. *The Legal and E-Commerce Environment Today* (Hardcover ed.). Thomson Learning. pp. 741 pages. ISBN 0-324-06188-9.

Palmer, C. (December 1998). *Using IT for competitive advantage at Thomson Holidays*, Long Range Planning Vol21 No6 p26-29 Institute of Strategic Studies Journal. London. Pergamon Press.

Reducing Risks, Protecting People, HSE's Decision Making Process, HMSO 2001, ISBN 0 7176 2151 0.

Report on the Causes of the Gulf of Mexico Tragedy, BP, 08 September 2010.
http://www.bp.com/genericarticle.do?categoryId=2012968&contentId=7064893

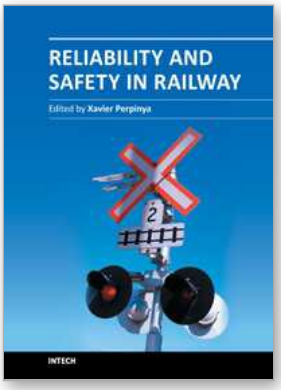
+Safe Version 1.2, *A Safety Extension to CMMi-DEV Version 1.2*, Defence Materials Organisation, Australian Department of Defence, March 2007.

SafeRelNet European Network of Excellence, www.mar.ist.utl.pt/SAFERELNET Guedes Soares, C. (editor 2010), *Safety and Reliability of Industrial Products, Systems and Structures*, CRC Press, PP:21-31, ISBN 978-0-415-66392-2.

*The Offshore Installations (Safety Case) Regulations 2005, Reprinted 2006,* The Stationery Office Limited.

*The Railways (Safety Case) Regulations 2000*, The Stationery Office Limited.

T430: *The Definition of VPF and the Impact of Societal Concerns*, Railway Safety & Standards Board, RSSB 2006, UK. *http://www.rssb.co.uk/*




**Reliability and Safety in Railway**
Edited by Dr. Xavier Perpinya

ISBN 978-953-51-0451-3
Hard cover, 418 pages
**Publisher** InTech
**Published online** 30, March, 2012
**Published in print edition** March, 2012

In railway applications, performance studies are fundamental to increase the lifetime of railway systems. One of their main goals is verifying whether their working conditions are reliable and safety. This task not only takes into account the analysis of the whole traction chain, but also requires ensuring that the railway infrastructure is properly working. Therefore, several tests for detecting any dysfunctions on their proper operation have been developed. This book covers this topic, introducing the reader to railway traction fundamentals, providing some ideas on safety and reliability issues, and experimental approaches to detect any of these dysfunctions. The objective of the book is to serve as a valuable reference for students, educators, scientists, faculty members, researchers, and engineers.



**InTech Europe**
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

**InTech China**
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821