European Commission
Fifth Framework programme
SAMRAIL

# D2.9.1: Synthesis of SAMRAIL findings



| | |
|---|---|
| Authorised by: | Ian Shannon, Atkins Rail |
| Reviewed by: | Hans Kuijlen, ProRail<br>Peter Mihm, DB<br>El Miloudi El Koursi, INRETS<br>Farha Sheikh, European Commission |
| Compiled by: | Swapan Mitra |
| Document ID: | SAMRAIL/SM/D2.9.1/V2 |
| Date: | 08 December, 2004 |
| Contract N°: | GMA2-2001-52053 |

| | |
|---|---|
| Type of document: | SAMRAIL Deliverable |
| Status: | Released |
| Confidentiality: | Restricted to personal use |
| WP allocation: | « WP 2.9» |
| Distribution: | SAMRAIL/SAMNET partners and EC |

History:

| | |
|---|---|
| Version 0: | September 24, 2004 first draft |
| Version 1: | October 5, 2004 includes comments from the reviewers |
| Version 2: | December 8, 2004 includes the Commission's comments |

Document Abstract: The results of the SAMRAIL technical work packages are analysed and synthesised identifying key issues and future directions.

List of Contributors (Alphabetical Order):
Farha Sheikh, DG TREN
Patrizio Grillo, DG TREN
All SAMRAIL members

Sponsor: This report reflects work which is funded by the European Commission under the competitive and sustainable growth programme of DG TREN. The work is related to SAMRAIL "Safety Management in Railways"

# EXECUTIVE SUMMARY

This report summarises the outcome of the research undertaken by SAMRAIL. It discusses the main findings, and lists the recommendations and outstanding issues.

The main objective of SAMRAIL was to develop a comprehensive and consistent safety management programme for the European railways, which could provide a basis for implementing the European Railway Safety Directive.

The work was organised into eight technical work packages, they analysed a specific set of requirements specified by the Safety Directive [1]. Their main aims were to identify the means necessary to implement these requirements.

The main conclusions of the survey of current practices carried out by SAMRAIL [4] were as follows:

- In line with other safety critical industries, the Safety Directive [1] has been suitably formulated and addresses all the important safety issues that an open, vertically separated and horizontally integrated railway of the EU could face.
- There is a sufficient base-line to develop the work planned by SAMRAIL on Common Safety Methods (CSM), Common Safety Targets (CST), and Common safety Indicators (CSI) and for safety certification and approval issues.

SAMRAIL has proposed a commonly agreed structure for the Safety Management System (SMS) comprising of a number of different elements and specifies requirements and guidance for each SMS element. The Guidelines [5] are intended to help duty holders in the implementation and on-going application of an effective SMS to meet the requirements of the directive. SAMRAIL recommends that the proposed Guidelines, approaches and processes are further developed through test and trial. It also identifies the steps which could be taken by the Commission and European Railway Agency to develop a SMS certification standard from the Guidelines.

To address the CSM related issues, a risk management approach is proposed along with a definition of the railway system and accident scenarios.

Two types of safety targets have been suggested, global targets for measuring member states' performance and safety levels for measuring performance of individual railway functions. A generic approach based on AEIF (European Association for Railway Interoperability) functional architecture has been proposed for apportionment of safety targets among the stake holders [7].

SAMRAIL has identified four categories of safety certification and approval processes, i.e. at component level, subsystem level, integrated module level and at service level. A Safety Approval Process is proposed with a suggestion for assessment methods [8].

SAMRAIL found that some of the CSI identified by the Safety Directive [1] are used by the member state railways to measure safety performance; however, the reference data and indexations of these CSIs need further consideration [11]. Many railway organisations have got adequate facilities to learn from these experiences, however, there is a need for developing a more integrated approach to organisational learning programme as proposed in [10].

The national safety rules are based on national standards and practice, and provide the basis for achieving the national safety targets. They are also are rooted in the respective safety culture, however, they can also pose technical barriers to open market [12]. The Safety Directive [1] recognises that the TSIs are insufficient to provide definitions of all aspects of system and operation, therefore, it recommends that, where necessary, complementary national safety standards could be applied. Under the Interoperability Directives the notification of all such standards are required. The Safety Directive [1] also requires notification of national safety rules. So far, notification of national rules has yet to start, and identification of national standards associated with the TSI implementation has been carried out by only a few member state railways. It is very difficult to find out which national standards have been notified.

SAMRAIL proposes an approach to develop common technical standards from the existing practices and through consultation with the stake holders so that migration to these from national standards could be made easy.

In SAMRAIL the roles of rules and regulations and their unification were also studied and they are found to be important for achieving safety performance. SAMRAIL proposes a rule management framework which could be used to improve the rule writing and implementation process [13].

While preparing this work, the stake holders were regularly consulted through SAMNET, the thematic network project, which helped to organise various meetings with different stake holders ranging from railway inspectorates from different member states, safety directors of railways to association of train operators and individual safety experts.

# CONTENTS

# 1 INTRODUCTION

SAMRAIL was prepared in response to the Smart Rail call for proposals (2.2.3/14 sub-task 2) and its objective was to develop a comprehensive and consistent safety management programme for the European railways, which could provide a basis for developing and implementing the European Railway Safety Directive.

SAMRAIL started on 1 February 2003, the technical work started soon after this and finished on 31 July 2004. The duration of the project was 18 months, and about 150 person-months were expended to complete this collaborative project. This work was fully funded by the Commission under the Fifth Framework Programme.

The SAMRAIL work was organised into eight technical work packages, comprising:

- WP2.1: Reviewed the state of the art in safety management, and identified how the safety approaches used in the European railways compare among themselves and with those used in other safety critical industries. This work provided the baseline for the rest of the technical work packages.
- WP2.2: Developed a set of guidelines for Safety Management System through consultation with the many European railway organisations and attempted to meet the requirements set out in the Safety Directive.
- WP2.3: Addressed the issues concerning Common Safety Method (CSM), and proposed an approach to qualitative and quantitative risk analysis.
- WP2.4: Addressed the issues concerning Common Safety Target (CST) and acceptable (safety) risk levels, and for risk apportionment.
- WP2.5: Addressed the safety certification and safety approval issues, including cross acceptance of subsystems and equipment in the European railways.
- WP2.6: Addressed the issues concerning Common Safety Indicators (CSI), in particular, developed a common process for incident and accident reporting and investigation and organisational learning.
- WP2.7: Reviewed the standards and good practices in the European railways, and methods used for checking their compliance.
- WP2.8: Addressed the railway operation issues, in particular the safety regulations and rules of the railways.

While preparing this work, the stake holders were regularly consulted through SAMNET, the thematic network project, which helped to organise various meetings with different stake holders ranging from railway inspectorates from different member states, safety directors of railways to association of train operators and individual safety experts. The main purposes of these meetings were to seek opinions of the stakeholders on crucial issues and to keep them informed the about the proposed solutions. The reviewers of SAMRAIL and the Commission were kept informed of progress.

The main deliverables of these work packages are as follows:

| Work Package | Identifier | Topics addressed |
|---|---|---|
| WP2.1 | D2.1.1[4] | Review of safety management approaches and reporting practices |
| WP2.2 | D2.2.2 [5] | Guidelines for the Safety Management System |
| WP2.3 | D2.3 [6] | Common Safety Methods |
| WP2.4 | D2.4 [6] | Acceptable Risk Levels |
| WP2.5 | D2.5.1 [8] | Safety Approval and Cross-Acceptance |
| WP2.6 | D2.6 [9]<br>D2.6.0 [10]<br>D2.6.1-A [11] | Accident and Incident reporting system<br>Organisational Learning<br>Position paper on Common Safety Indicators |
| WP2.7 | D2.7.1 [12] | Standards and Best Practice |
| WP2.8 | D2.8.1 [13] | Regulations, roles of rules and their unification |

These deliverables have been reviewed by an independent board of reviewers set up by SAMRAIL and also by the Commission's officers from DGTREN.

## 1.1 Objectives

The objectives of this document are to identify the main findings of SAMRAIL and discuss how they can be used to support the Safety Directive [1]. Based on these discussions, a set of recommendations are made with suggestions for their implementation. It also aims to propose an approach to address the outstanding issues identified in SAMRAIL.

## 1.2 Structure of this document

The findings of the SAMRAIL technical work are summarised in the next section. In Section 3 the recommendations and suggestions for their implementation are discussed. Section 4 is devoted to the outstanding issues and ways to address them.

# 2 FINDINGS OF SAMRAIL

## 2.1 General

The variety of Community legislations on railways have produced a myriad of safety requirements with which it is often difficult to comply with and safety approval of a service or operation, the Safety Directive [1] is a timely legislation. There are different national rules. Safety approval is one of the hardest hurdles for open market.

The SAMRAIL work packages were planned to address the implementation issues of the Safety Directive. Each of these work packages focussed on a specific set of requirements specified by the Safety Directive [1] and aims to identify:

- where possible, the means necessary to implement the planned objectives;
- where the objectives entail complex issues and it was not possible to resolve them and offer a suitable solution, SAMRAIL has proposed a course of actions to be undertaken through SAMNET and other programmes.

| **Title** | **Safety Directive [1] Requirements** | **Objectives** |
|---|---|---|
| WP2.1: Analysis of existing methods | *Common regulatory framework for railway safety; overcome the differences in safety principles, approach and culture in railways* Clause (1) & (2) | To identify how other safety critical industries have addressed these issues (needed in the Call for Proposal ); to assess the differences between the national principles, approaches and cultures, and identify if there are any examples where they have been bridged or harmonised; to suggest approaches and the base-lines for overcoming the differences |
| WP2.2: Safety Management System | *Implementation of Safety Management System* Clause (11) & Article 9<br>*Requirements on SMS* Annex III | To specify guidelines for developing the SMS and seek consensus from the stake holders; to identify what can be contributed by other work packages to achieve the overall objectives of the SMS |
| WP2.3: Risk analysis approach | *Gradual introduction of CSTs and CSMs, ..tools for assessment of the safety level and the performance of the operators* Clause (8);<br>*To describe how the safety level, and the achievement of safety targets and compliance with other safety requirements are assessed by elaborating and defining risk evaluation and assessment methods…* Article 6 | To identify risk evaluation and assessment methods suitable for assessing safety levels and checking compliance with safety requirements; to identify the tools for assessment; to specify the process for introducing CSMs from the base-lines identified in WP2.1 |
| WP2.4: Acceptable risk levels | *Draft CSTs and draft revised CSTs shall be drawn up… CSTs shall define the safety levels that must at least be reached by different parts of the railway system and by the system as a whole in each Member State* …Article 7 | To specify a set of guidelines for specifying CST; to propose a scheme for apportionment of safety level to different parts of the railway system |

| | | |
|---|---|---|
| WP2.5: Safety approval and Certification | *Safety certificate* …. Article 10<br><br>*Safety authorisation of infrastructure managers.*…. Article 11<br><br>*…methods for assessing conformity with requirements in safety certificates and safety authorisations issued in accordance with Articles 10 and 11*… Article 6<br><br>*Requirements include: application of TSIs and national safety rules, acceptance of staff's certificates and authorisation*<br><br>*To place in service the rolling stock used by the railway undertaking.*…Article 10<br><br>*… safe design, maintenance and operation of the railway infrastructure including, where appropriate, the maintenance and operation of the traffic control and signalling system* … Article 11(b) | To specify a process for safety certification (and authorisation) of railway systems and their elements and acceptance of services; to identify how a common set of acceptance criteria can be formulated from the base-line identified in WP2.1; to propose a method for assessing conformity with the Safety Directive's certification/authorisation requirements |
| WP2.6: I&A reporting and Organisational Learning | *Accident and Incident investigation* Article 19<br><br>*It is thus necessary to establish common safety indicators (CSIs) in order to assess that the system complies with the CSTs and to facilitate the monitoring of railway safety performance. However, national definitions relating to the CSIs may apply during a transitional period and due account should therefore be taken of the extent of the development of common definitions of the CSIs when the first set of CSTs is drafted.*… Clause (9)<br><br>*… shall collect information on common safety indicators (CSIs) through the annual reports of the safety authorities as referred to in Article 18*…. Article 5(1) | To propose a common approach to A&I reporting and for learning from the experience; to identify common set of CSI for monitoring safety performance and access safety levels |
| WP2.7: Standards and best practice | *National safety rules, which are often based on national technical standards, should gradually be replaced by rules based on common standards* Clause 10<br><br>*…infrastructure managers and railway undertakings, obliging them to implement necessary risk control measures, where appropriate in co-operation with each other, to apply national safety rules and standards … Article 4(3)* | To survey the safety standards and best practices currently in use by different railways; to check how they map on to TSIs; to identify a practical method for checking compliance with the standards |
| WP2.8: Regulations, roles of rules | Same as above | Rules and regulations, often expressed formally in rulebooks, are a representation of the safety culture. A common framework to implement rules is proposed to support the requirements of the Safety Directive [1] |

In particular, WP2.2 addresses the requirements for managing some of the main processes that are needed to establish the common framework specified in Annex III of the Safety Directive [1]. The management of the processes is mainly concerned with the provision of adequate resources, control and monitoring against the plans, timely reporting, and devising corrective actions. Actual details of the processes, such as specific methods and tools, application requirements, implementation details etc. are addressed in WP2.3 to WP2.8. These processes are identified in the Safety Directive [1] as:

- Annex III of [1], *Plans and procedures for* setting and *reaching qualitative and quantitative (*safety*) targets*, these are addressed in WP2.3 and WP2.4
- Article 6 of [1], CSM, risk evaluation and assessment method addressed in WP2.3
- Article 7 of [1], Approach to identify and set the CST addressed in WP2.4
- Articles 10 and 11 of [1], Certification and safety approval processes addressed in WP2.5
- Article 5 of [1], Processes for identifying and setting CSI and Accident and Incident reporting addressed in WP2.6
- Basis for establishing common principles, approaches and culture; it is believed that these safety attributes are manifest in the prevailing standards, best practices and safety rules (rulebooks). These issues are addressed in WP2.7 and WP2.8.

However, it does not address the regulatory or administrative issues concerning European Railway Agency (ERA) or legislative issues.

## 2.2 Results of Work Packages

The findings of the work packages are summarised below.

### *2.2.1 WP2.1: Analysis of existing approaches*

This work was carried out under the leadership of TIFSA, and reported in SAMRAIL deliverable D2.1.1 [4]. The main findings of this work are as follows:

- The European railways are good at safety management of their operations. Although they do not have an identifiably separate formal Safety Management System, such as that required by the EU Safety Directive, they seem to be adequate for the safety of the services. The objectives of the Safety Directive [1] and its safety certification framework are similar, in many respects, to those currently achieved and in use by maritime and civil aviation sectors.
- The Safety Directive [1] provides a suitable base-line for developing a common safety management system framework for the EU railways. The directive identifies its main elements, namely: safety policy, responsibility, accountability, risk assessment and evaluation, communication and information provision, learning from accidents and incidents, emergency managements. However, the following additional elements identified in the safety management approaches of nuclear and process control industries could also be useful:
    - Management of inspection, maintenance and modification processes

- Proactive learning from experience and benchmarking
- Management of rules and procedures
- Management of commitment, conflict resolution and motivation
- Interface design, work layout and ergonomics
- Maintenance of hardware.

- A common framework for SMS among the IM and RU is essential for supporting vertical separation and an open market policy of the Community. A similar code of practice, ISM code, was successfully introduced in the maritime sector a few years ago.
- The railway infrastructures of the member states are not only technically incompatible, their safety requirements and assurance processes are often very different. In order to support horizontal integration the EU has introduced two inter-operability directives, but only a handful member states have managed to transpose them into their legislation. For horizontal integration, a uniform implementation of the TSI directives throughout the EU railways is needed. Some special bilateral arrangements exist between member state railways for specific inter-state operations, but there is no common policy on this. The maritime and civil-aviation sectors have managed to achieve horizontal integration through international agreements and mandatory codes.
- With regard to common risk analysis approach, it was found that the risk assessment and evaluation processes are well established and they are common to all industries. The use of standard techniques and tools in the railway sector require special knowledge and their effectiveness depends upon experience. However, to date the collective experience on inter-state operations can be a good starting point for developing CSM. The need for a common approach to risk mitigation measures is also identified, this will save individual railway organisations carrying out expensive safety justification and demonstration exercises.
- The CENELEC norm EN 50126 [2] addresses the approach for specify acceptable safety risks, it provides the base-line for the work package WP 2.4. In contrast with maritime and civil aviation sectors, where the target level of safety is measured in terms of hull losses, the railways tend to measure this in terms of human fatalities and injuries. Some railways have formally set their target safety levels and devised means to demonstrate them, these target levels are similar to those identified in the Safety Directive. Whereas the methods for calculating individual risks in railways are well developed, the issue of societal risks is seldom addressed. The method developed by the civil aviation sector to calculate acceptable societal risks could be used.
- The work package WP2.5 on safety approval and cross acceptance of equipment is important for implementing the safety certification and approval requirements of the Safety Directive. At present, the certification and cross acceptance policy in the EU railways are very limited. There are different national regulations and rules and different safety assessment criteria and certification processes. The civil-aviation model based on product and process certification where the authorities certify aircraft, their manufacturers, and their repair and maintenance processes could be used to improve this situation.

- Some of the requirements identified in the Safety Directive [1] for incident and accident reporting can be met by the UIC Accident database. However, it was found that many member state railways have developed more elaborate databases for their own use which could also cater for most of the Common Safety Indicators (CSI) identified by the Safety Directive. Many railways are aware of the importance of organisational learning from the incidents and accidents. It is deemed very important by many railways, however, no clear policy has emerged on its implementation at a national or European level.
- The base-line for the work package WP2.7 is the European railway safety standards in use, (several of which are still in pre-norm stage) and the relevant requirements of the TSIs (HST and conventional trains). The safety standards of space, nuclear and process control industries provide useful direction for improving safety and demonstrating compliance.
- The safety regulations and rules are very important elements of the railways; they represent the safety culture and customs of the organisation. They could be categorised into hard-wired rules, technical forcing functions, administrative standards, self-control and social group regulations. To understand their role it is important to identify the goal of rules, assessment needs of a rule from management perspective, and development, implementation, auditing and modification processes.

The overall conclusions of this work were as follows:

- In line with other safety critical industries, the Safety Directive [1] has been suitably formulated and addresses most of the important safety issues an open, vertically separated and horizontally integrated railway of the EU could face.
- There is a sufficient base-line to develop the work planned for CSM, CST, and CSI and for safety certification and approval.

### *2.2.2 WP2.2: Safety Management System*

The Safety Directive [1] is proposing to establish a common and transparent regulatory framework for the European railways and as a part of this it requires Railway Undertakings (RU) and Infrastructure Managers (IM) - the duty holders) - to prepare, implement and maintain formal Safety Management System (SMS). It introduces the concept of common requirements for, and common elements of an SMS.

These basic concepts were further developed in this work and concluded that [5]:

- An SMS is an organisation’s formal arrangement, through the provision of policies, resources and processes, to ensure the safety of its work activity. An effective SMS helps the organisation to identify and manage risks effectively. It allows an organisation to demonstrate its capability in achieving its safety objectives and in meeting regulatory requirements.
- Evidence of an effective SMS provides confidence in an organisation’s safety management capability which in turn helps in the safety assurance of the systems and services the organisation controls and provides.

This work proposes a commonly agreed structure for the SMS comprising of a number of different elements and specifies requirements and guidance for each SMS element. The

guidelines [5] are intended to help duty holders in the implementation and on-going application of an effective SMS, to meet the requirements of the directive.

It is considered crucial that the SMS of each duty holder specifically addresses all types of risk to which it is exposed. It recognises that an organisation faces essentially three different types of risk to its operations:

- Internal risks, i.e. those associated with activities and locations for which the organisation is solely responsible.
- External risks, i.e. those originating from systems, people or organisations and processes that are outside the organisation's control.
- Shared risks, i.e. risks associated with activities or locations for which there are shared responsibilities rather than sole ownership; to manage such risks the organisations have to ensure that compatible approaches are used.

It requires that the SMS identifies all its internal risks, specifies the safety target levels associated to these, and explains how the internal risks are managed. Furthermore, it requires the SMS to explain the approaches taken to minimise the external risks, and to identify the shared risks and to explain how they would be controlled.

The following table summarises the requirements for the each SMS elements, the SMS guidelines on how these requirements could be met is provided in [5].

| No | Element | Requirement |
|---|---|---|
| 1. | Nature and Scope of Duty Holder's Business | Duty holder to identify the nature and scope of their business and the risks associated with their business operations. They should be aware of their safety management responsibilities as required by Article 4.2 of the Safety Directive [1] and other national requirements. |
| 2. | Safety Policy | Senior Management to provide a clear statement of its commitment to ensure safety. This commitment should be effectively communicated throughout the organisation and should be apparent in the visible actions of management, and in provision of processes, procedures and resources. The organisation's safety objectives to include its safety target level and arrangements for managing safety with other duty holders. |
| 3. | Organisational structure and Responsibilities | Duty holder should establish and maintain clear and unambiguous lines of authority, accountability and responsibility for ensuring safety at all levels within the organisation. Responsibilities for interfacing with other organisations, such as safety authorities, IM and other RU, should be identified and properly integrated within the line management of the organisation. |
| 4. | Competence, Training and Fitness | Duty holder to ensure that its employees have appropriate experience, knowledge, skills, abilities and fitness to discharge their responsibilities. Their competence should be regularly evaluated and any identified deficiencies should be addressed through training, recruitment and/or organisational change. All necessary arrangements should be in place to help with the continuous improvement of their skills. |
| 5. | Risk Management | Duty holder to have in place procedures for identifying areas of risk throughout the organisation, assessing it and determining effective control measures to reduce it. Risk assessment should be carried out using the CSMs, and residual risks should be consistent with CSTs. |
| 6. | Safety Assurance | Where risk within the duty-holder's overall area of responsibility, is not under their direct control, they must ensure that such risk is appropriately managed. Duty holder should put in place procedures to ensure that such activity is undertaken in accordance with their overall SMS, and appropriate risk levels are achieved. Such consideration may require contractual commitments to be placed on those undertaking such activity. |
| 7. | Incident and Accident Reporting and Learning | Duty holder to put in place procedures for reporting and investigating A&I events. Such processes should encourage reporting amongst staff. Duty-holder should also have procedures for learning from A&I events, lessons from these should be disseminated throughout the organisation, and to others. |
| 8. | Emergency Management | Duty holders to put in place a framework and generic procedures for managing response in the event of emergencies and specific procedures for managing foreseeable emergencies. These procedures should address the minimisation of risk in the event of emergencies, stabilisation of the railway and its operation, sustaining of degraded operations, and recovery to normal operations. |
| 9. | Safety Communication and Information Integrity | Safety communications and information to be defined and documented. Duty holder to ensure that they are aware of the criticality of the various communication issues. The integrity of safety communications and information should be managed as appropriate to this level of criticality. All safety related documentations should be under strict change control. |
| 10. | Management of Rules and Standards, including Compliance | Duty holders to have procedures in place for the identification of legislation, rules, standards and technical requirements relevant to their work activity. They should have in place procedures to ensure that these requirements are complied with. Procedures should also address management of non-compliances which should be undertaken according to a risk-based process consistent with the organisations overall SMS and risk criteria. |
| 11. | Monitoring, Auditing and Annual Reports | Duty holder to have in place procedures for the monitoring, and audit of the SMS. Such review should be undertaken regularly. It should contain procedures to ensure that corrective measures identified via audit and monitoring are fed back and implemented. Duty holder to prepare annual safety reports. |

### *2.2.3 WP2.3: Risk analysis approach summary*

The Safety Directive [1] needs Common Safety Methods (CSM) which could be used to assess "*safety level, and the achievement of safety targets and compliance with other safety requirements*". It requires that draft CSMs be based on "*an examination of existing methods in the Member States*". It is believed that in time the draft CSMs will be revised and adopted for use. A first set of CSMs, covering at least the "risk evaluation and assessment method" shall be developed and adopted by 2006. This work provides the basis for developing the draft CSMs. It is based on the findings of the survey of risk assessment methods carried out by WP2.1. The main findings of this work [6] are as follows:

- Risk management approaches used by the railways are very similar to each other. The main steps of these approaches comprise:
    - identification of hazards[†],
    - evaluation or analysis of risks associated with these hazards
    - identification of control measures
    - selection and performance of control measures, and risk minimisation
    - contingency plan or reactive measures for these hazards
    - change management
- Generally, a Bow Tie Model is used to explain these steps. The hazardous event occupies the centre of the Bow Tie. Its left hand side contains the causes that potentially lead to the hazardous event. Also shown on this side are the controls or barriers to the hazard, they are also known as preventative controls. The right hand side of a Bow Tie contains the event tree which shows the various outcomes that can potentially occur and the controls or barriers that are in place to limit or reduce their consequences. These are also called reactive controls or mitigation measures. Clearly the preference is for effective proactive control measures, but reactive control is also essential to minimise harm in case a hazardous event accidentally slips through.
- A common system definition is necessary for ensuring that hazard identifications and risk evaluations carried out by different railways are consistent and comparable. Presently, scenarios used to identify hazards are not consistent with each other. This work has proposed a definition of railway system, identifying its different elements, functions and boundaries. A list of commonly occurring accident scenarios is also proposed.
- Generally, the risk management is initiated at the system development stage, where designs are analysed for the planned operations under normal, degraded and emergency conditions. The results of these, along with the operationally ready system, are passed on to the duty holder. The hazardous events encountered during operations and maintenance phases are handled using the same risk management approach.

[†] For definitions of hazard and risk see SAMNET glossary [14]

- This work also emphasises that risk management is also required for the post-operational phases of the railway systems, namely renewal, extension and decommissioning phases.
- Three types of risk analysis methods (quantitative, qualitative and semi-qualitative) are commonly used. It is believed that there is no uniformity or consistency in their applications. It was found that, for a given hazardous event, different organisations use different risk analysis methods, and if even when they use the same method, they apply them with different degrees of rigor.
- Although it is desirable to devise control measures which completely eliminate the risks, it is not always practicable. Different selection criteria of control measures have been developed to address different societal views on risk acceptance. Most commonly used risk acceptance principles used by the main line railways are Globalement Au Moins Equivalent (GAME) meaning globally at least equivalent, Eisenbahn-Bau-und Betriebsordnung (EBO) and as low as reasonably practicable (ALARP). Whereas GAME and EBO are similar in many respects, i.e. they require comparison of risks with those of other similar systems in use, ALARP requires cost benefit analysis of the control measures.

It is believed that the common Risk Management approach identified here could be used as the basis for developing the draft CSM. To facilitate the common hazard identification, this work is proposing a common definition of the railway system which identifies its main entities, subsystems, boundaries and interfaces. It has also collated an extensive list of accident scenarios which could be used as the base-line in the draft CSM.

The techniques and tools commonly used in risk management are also identified. Some of these are specifically designed to address operational and maintenance issues, they include:

- Workplace Risk Assessment and Control (WRAC)
- Human Error Analysis (HEA)
- Hazard and Operability Study (HAZOP)

### *2.2.4 WP2.4: Acceptable risk levels*

The Safety Directive [1] stipulates that the Common Safety Targets will be set by the European Railways Agency (ERA). This work therefore concentrated on the issues related to the development of CSTs and their roles in safety management. After reviewing different methods of specifying CST and comparing their relative values, it proposes a set of guidelines for specifying safety targets, and a scheme for risk apportionment. The latter is based on the functional decomposition scheme proposed by AEIF. Definitions and other considerations mainly derived from the Safety Directive [1] have been taken into account.

The main findings of this work [6] are as follows:

- The decision to set a Common Safety Target (CST) is going to be based on political criteria, possibly guided by financial and economical principles and state-of-the-art technology and science. This should ensure that the targets are reachable and affordable by Member States.

- To specify and analyse the risks associated with the types of railway operations identified by the Safety Directive [1], a precise definition of the railway system and its boundaries are required.
- In general safety targets can be derived from accidents and their consequence data over a fixed period of time. However, for a better evaluation of safety performance, statistical inference should be drawn from long term data where all types of events, especially low frequency and high consequence events, are properly represented and accounted for.
- According to the Safety Directive [1], CSTs shall define safety levels expressed in risk acceptance criteria for different categories, i.e. for passengers, staff, level crossing users, trespassers and for others.
- Safety levels associated with societal risks is also identified as one of the CSTs. Unfortunately, the EU railways have yet to reach a consensus on the definition of societal risks, and therefore, for the purpose of this work societal risk is regarded as a measure of the frequency of accidents which lead to multiple fatalities. Therefore they could be covered by some of the categories identified above and there will be no further investigation on this issue.
- A CST related to minor injury statistics could be a useful measure of safety performance because minor injury events are more abundant, and are often indicative of inherent problems which could potentially lead to serious accidents. However, the EU railways should agree on a common definition for minor injuries so that a uniform measure could be specified.
- The indexation or reference units to be used for specifying the safety levels could be train kilometres. However, other meaningful units could be equally used, for example, it will be more appropriate to index staff fatalities and injuries by working hours, and fatalities and injuries of level crossing users by frequency of level- crossings.
- Two sets of CSTs have been identified:
    - Global CSTs for measuring performance of the member states: these are to be based on overall statistics of the railway networks and are useful for benchmarking purposes.
    - Safety levels for measuring performance of individual railway functions or operations, such as “Support and guide trains” or “Load passengers”, are useful for prioritizing and planning improvement tasks. They could be used as acceptance criteria for existing equipment (e.g. in-use rolling stocks), or for new technologies and products. They could also be used to identify safety targets for the individual organisations, such as RU or IM, however to achieve this, a detailed functional analysis of the railway operations has to be carried out to identify risks associated with train operation or infrastructure management.
    - These types of CSTs would be helpful for the networks to specify the requirements for train operation and acceptance criteria for equipment and products.
- Common Safety Methods, especially hazard analysis and risk assessment approaches, could be used to derive safety targets for technical installations as well as for operational procedures to ensure railway safety.

- A generic approach to functional decomposition, based on AEIF "railway architecture", has been proposed for the apportionment of CSTs. It requires detailed analysis of each function:
  - to ascertain to which duty holder could be assigned responsibilities
  - to identify the associated hazards and their possible consequences and associated safety indicators
  - to collect historical data on the consequences and safety indicators and calculate the target statistics.

### *2.2.5 WP2.5: Safety approval, Cross-Acceptance and Certification*

The base-line for this work was drawn from the results of the survey on existing safety certification and approval processes, and the safety approval policy specified in the Safety Directive. The Safety Directive [1] has specified a certification and authorisation based approval policy, which is designed to overcome the barriers posed by different national regulations. It specifies the processes for granting access to an RU and for permitting IM to manage and operate a railway infrastructure and identifies the requirements for safety certification and safety authorisation. The base-line information is used as the basis for developing a generic Safety Approval Process (SAP). The objective of the SAP is to allow easy migration to the Safety Directive [1] approval regime. The main findings of this work [8] are as follows:

- As per the Safety Directive [1] approval policy, to operate its trains on a railway infrastructure an RU will require a certificate for its SMS and certificates which show that it meets the network specific requirements, e.g. compliance with TSI and national safety rules, staff competence, and rolling stock authorisation. The latter requires certificates which show that the rolling stock meets the appropriate TSIs or national rules.
- Similarly, to get the permission to manage and operate an infrastructure, an IM will be required to have a certificate for its SMS and authorisation confirming that it meets specific requirements for safe design, maintenance and operation of the infrastructure, e.g. compliance with TSIs, national rules, and staff competence.
- The existing safety approval processes, though similar in structure, are implemented in many different ways, for example, some are based on compliance with prescribed national standards and others are based on safety-case approach. They also do not require separate approval for the organisation's SMS. In addition, there is also a great deal of disparity in the implementation of TSIs and notification of national safety rules. In many member states the national safety rules do not take into account the applicable directives, for example those concerning inter-operability issues. With regard to staff competence not all organisations have formal requirements for certification. The competence requirements for the safety critical staff are specified by many but not all at the same level of detail.
- This work has identified the following four categories of safety certification and approval processes from the existing approaches which can be used to implement the Safety Directive's certification and authorisation requirements. They comprise:
  1. Certification at component level, e.g. a pantograph or a signal head

2. Certification at subsystem level, e.g. a rolling stock, signalling system, staff (e.g. drivers, signalmen)
3. Certification of integrated modules including railway organisations and railway systems, e.g. RU (through certification of its SMS), or arrangements for the authorisation of rolling stock for specific infrastructure (i.e. vehicle acceptance).
4. Approval to operate a service, e.g. granting permission to an RU to run trains on a specified infrastructure, or authorising an IM to manage and maintain the specified infrastructure.

- This work proposes a generic approach for representing these processes which identifies and explains:
  - the 'actors', the participating organisations, and their roles in certification
  - assessment criteria for certification or approval, for instance, those related to conformity with standards, to compliance with safety rules, and to risk based approach; it may also include criteria on the quality of the evidence (e.g. quantitative analysis, independent assessment)
  - stepwise process of certification, starting from application for a certificate to renewal and revocation of certificates
  - the issues concerning cross-acceptance of certificates at component, sub-system and organisation levels are identified and discussed
- The above four SAPs (Safety Approval Processes) support each other hierarchically: component certificates are used as evidence to seek certification of sub-systems, sub-system certificates are used as evidence in integrated modules and railway system certification, and finally the integrated modules certificates are used by RU and IM to seek permission to operate. The requirements of the higher levels of certification provide the basis for setting the assessment criteria for the lower level certification.
- The Generalised Assessment Method [15] developed under the CASCADE project, could be used to implement the SAP. This approach is suitable for checking compliance with the common risk-based criteria.
- The risk based criteria, could provide a common basis for implementing the SAP. They are generally expressed as 'safety principles' for determining acceptable risks levels. For the lower level SAPs, i.e. component and sub-system levels, these safety principles could be used to set their Tolerable Hazardous Failure Rates as their acceptance criteria. The safety principles could also be used to set safety target levels for the railway systems, operations and services. There are three apparently different safety principles, GAME, MEM and ALARP, and they may converge in terms of results when established standards for safety are applied.
- This work recognises that cross-acceptance of certificates is essential for implementing the Safety Directive's approval policy, and this would be needed at the component and sub-system levels. The TSI and inter-operability rules provide a general basis for implementing this policy, however, in practice, different application, environment and national rules could require additional assessment before a component or sub-system's safety certificate is accepted. With respect to the cross-acceptance of rolling stock between Germany and France (ICE3 and POS), the problem is that nowadays common

standards do not exist, as has been explained previously, many points are missing in the TSI. In order to achieve cross acceptance a preliminary safety case has been made. This safety case describes the differences between the standards for each type of rolling stock and the way to solve the problem. An agreement is made on each solution (of course, France and Germany cross-accept the rolling stock certificates delivered by each other). Nevertheless tests are mandatory in order to assess compatibility with the two infrastructures.

### *2.2.6 WP2.6: Incident and Accident Reporting and Organisational Learning*

The Safety Directive [1] has specified a detailed policy on incident and accident investigation and reporting. It also emphasises importance in "further improvement of rail safety", and identifies a set of Common Safety Indicators which could be used "to assess the system complies with the CSTs and to facilitate the monitoring of railway safety performance".

This work was planned to address the migration issues related to these Safety Directive's [1] policies. A survey of current practices in seven member states including the description of the UIC's I&A database and EuroStat requirements [2] were carried out and requirements of the Safety Directive [1] were analysed. The main findings of this work are identified below:

- The member state railways consulted in this work have well established I&A investigation and reporting processes. They are based on formal policies and implemented through codes of practice, procedures and work instructions. The collected information is used by the railways to measure performance and improve safety [9].
- The accidents (fatalities and major injuries) are invariably reported to the safety authorities and included in the national statistics, however, reports on minor injuries and incidents are not generally shared [9].
- The organisations have got adequate facilities to learn from these experiences, however, usually the lessons learnt from these events are not shared among the railways. There is a need for developing a more integrated approach, organisational learning programme, which could be beneficial to all stake holders and help to meet the Safety Directive's objectives [9].
- This work [11] has drawn the following conclusions on the Common Safety Indicators identified by the Safety Directive[1] :
    - Specific set of CSIs are needed to monitor railways safety performance against the safety objectives set out by the specified CSTs identified by SAMRAIL
    - The CSIs relating to accidents are most appropriate for measuring relative safety performance as other types of CSIs are not uniquely defined, and not reported and analysed uniformly
    - CSIs provide the basis for improving safety performance, for example incident investigations, identifying their precursors and corrective measures
    - Historic data on CSIs could be used in specifying risk profiles of their associated hazards

- Safety management related indicators could be used to check the compliance with the organisation's Safety Management System
- More work on identifying indexation and normalisation of event related data, better classification of CSIs relating accidents to help with safety performance improvement, and research on standardisation of indicators

- With regard to learning from incidents and accidents, this work [10] found that:
  - The present arrangements in the member state railways are not adequate, they are weakened by the recent reforms which fragmented the national railways; new and improved learning arrangements which extends over all 'fragments' are necessary to restore their effectiveness.
  - Piecemeal learning processes currently in use are generally ad-hoc and symptomatic, often aimed at individual events. Such events are not recorded effectively in organisational memory, and thus not fully supported by management, and therefore often forgotten after the involved persons have moved. In short, piecemeal learning is rather a barrier for organisational learning and basically ignorant to the phenomenon of organisational memory.
  - Organisational learning is a systematic process through which 'operational surprises' are identified and analysed, corrective actions are devised and implemented, and the effectiveness and impact of the corrective actions are monitored. An operational surprise occurs when somebody or some monitoring system detects operational conditions that were not anticipated and might lead to an unsafe state.
  - The primary objective of organisational learning is to prevent I&A events recurring anywhere in the railways. The facility that provides OL is called 'Learning Agency': its implementation is a responsibility of appropriate line management. Data collected, processed and stored for this purpose also provided a sound basis for defining meaningful safety indicators.
  - Lessons learnt through organisational learning are captured in learning products that become part of organisational memory: the accessibility of this organisational memory is necessary in order to retrieve these lessons for reuse and further learning.
  - Lessons to be learned from a given event could be different for different stakeholders; opportunities to learn effectively will also be different. Some risks identified through learning from accidents or incidents might be better controlled by another stakeholder. All these considerations indicate the necessity to conceive organisational learning from railway-related accidents and (near-miss) by and for the European railways in order to meet the inter-operability objective.

### *2.2.7 WP2.7: Standards and Best Practice*

The railways standards and best practices were developed over the years to provide safe and reliable services. The national safety rules are based on these standards and together they provide the basis for achieving the national safety targets. As observed by the Safety Directive, these standards were developed on 'national lines', were based on 'technical and operational concepts'. It is also recognised that the national safety standards and best practices are rooted in the respective safety cultures, and they can pose technical barriers to open market. The

Safety Directive [ý1] expects that this situation will improve with gradual replacement of national standards with common standards based on TSIs. This work [12] addresses the migration issues related to national to common standards.
A survey of existing EU and national technical standards and the approaches used to comply with them was carried out. The experience gathered from their usage is analysed to identify the gaps and barriers and ways to overcome them. The main findings of this work is summarised below:

- The Safety Directive [1] recognises that the TSIs are insufficient to provide definitions of all aspects of system and operation, therefore, it recommends that, where necessary, complementary national safety standards could be applied. Under the Interoperability Directives the notification of all such standards are required. The Safety Directive [1] also requires notification of national safety rules.
- So far, notification of national rules has yet to start, and identification of national standards associated with the TSI implementation has been carried out by only a few member state railways. It is very difficult to find out which national standards have been notified.
- Commonly used methods for deriving tolerable risk levels from the EU and international norms have been reviewed. It is suggested that acceptable risk levels could be proposed in a quantitative form by using the existing risks cited in literature.
- In setting the CSTs the acceptable risk levels associated with individual risks and collective risk should be considered; individual risk budget for a railway operation can be determined using MEM principle and for collective risks ALARP principle can be used.
- A risk budget can be set per unit of track kilometre and per unit of rolling stock in order to give manufacturers and operators the possibility to fulfil the risk requirement
- Compliance with standards and assessment against standards were analysed, the procedures developed under CASCADE [15] and ACRuDA [16] projects for this purpose were found to be useful.

### *2.2.8 WP2.8: Regulations, roles of rules and their implementation*

The safety regulations and rules are important for achieving safety performance. In this work the roles of rules and regulations and their unification are studied. For this purpose, a framework for safety rule management was developed and tested through case studies. The main findings of this work [13] are summarised below:

- The railways are subjected to a hierarchy of rules, procedures, regulations, and work instructions. The highest level of these are EU directives and national laws, and below this level, are the regulations formulated by the national railway bodies to help with implementation of the law. The safety rules are formulated to help the railway organisations to put the regulations into practice. The next level is the *operational procedures and goals* relating to safety, covering all business processes and states of the railway system (e.g. construction, operation, maintenance, emergencies). At the level of the work-floor these operating procedures are translated into *work instructions*, which govern the minute-to-minute behaviour of people working on the system (traffic controllers, drivers and train crew, maintenance crews, etc.).
- Three different types of rules are identified:
  - Performance goals type rules are specified in terms of specific risk targets (e.g. risk contours around marshalling yards handling dangerous chemicals, target levels of incidents or accidents) or more general goals such as ALARP or GAME

  - Process rules include requirements to consult with a specified set of people when an emergency situation arises in order to decide how to handle it.
  - Action rules are specified in terms of 'If – Then' statements prescribing exactly how people shall behave, or how hardware shall be designed or tested.
- The rule management system is based on a framework which consists of a set of connected activities related to planning, writing, implementation and monitoring of rules. The framework also includes the links to higher levels of management processes, such as an overall safety management system. Finally, the framework incorporates links to external activities such as regulations from the EU, national regulation, labour union agreement etc. The framework was improved through different case studies in member state railways.
- The national case studies revealed that a large knowledge-base is available in the railway organisations. Unfortunately there are no formal processes in place to retain this organisational knowledge.
- In general, it seems that there is a lack of systematic risk identification and analysis at a formal level. These are especially necessary for those rules where the responsibilities are shared among several organisations.
- The changes in the railway sector with the monopolies disintegrating into several organisations with different responsibilities have revealed a stronger need for formalised communication and cooperation. The results show that the issue of cooperation and new ways of communication between the new organizations is important and not yet resolved.
- In the present time, the rule writing process is quite complex, expensive and time consuming because the responsibilities between different individuals are not clearly defined, and criteria for assessment and the qualities needed by staff required to comment are not available. This shortcoming also exists at the higher levels, e.g. formulation of laws and regulations at the member state levels.
- One formal way of monitoring and evaluating the use of rules is through the information from the incident and accident databases, which, however, cover only rule violations, not rules used in a broader sense. The continuous systematic use of investigation and evaluation of I&A events is needed to ensure organisational learning. The work of WP 2.6 on I&A reporting systems addresses this issue.
- The results of the informal monitoring and evaluation of the rules reveal that rule violations are happening every day. The violations could be related to inappropriate handling of administrative procedures or non-compliance in executing the rules, which may be due to e.g. outdated rules or personal gain in acting different from the rules. Also, there are several actors involved in the implementation of rules, which entails varying interests and a basis for conflicts when the rules are to be executed.
- It was found that there are several informal ways of handling enforcement of the rules, which are carried out through training. However, there is no tradition of escalating these problems to a higher level in the organisation, in order to get systematic enforcement proposals.
- Monitoring of the compliance, evaluation of the effectiveness of rules and enforcement where necessary are not coordinated properly, and in the case of the infrastructure manager, with the contracts with maintenance contractors, inspection and enforcement does not take place as often as it ought to.

# 3 RECOMMENDATIONS AND SUGGESTIONS FOR IMPLEMENTATION

| No. | Recommendation | Suggestion |
|---|---|---|
| 1. | The Safety Directive [1] is initiating a major change in the ways the safety of the railways are managed, such regulatory and cultural changes will require the involvement of all stake holders and their staff in this process. Following the experience of other transport industries, an awareness drive about the Safety Directive [1] should be launched to inform the railway community about its objectives, benefits, migration policy, and impacts on various aspects of the business. | Dissemination through publication and presentation on general and specific issues, and to tailor these for specific groups of workers, e.g. safety managers, signallers and drivers, safety authorities and their staff. |
| 2. | More explanation is needed on the certification policy specified in Article 10 and 11, e.g. how part A and B are related, how this policy will be implemented, how it will be supported by assessment and evaluation. It is also necessary to explain how the migration from the existing schemes, e.g. those based on safety case, will be carried out. | To develop a detailed certification process in collaboration with the national safety authorities, and consultation with the duty holders. This could be included in the scope of ERA's work programme Activity N$^{o}$ 2. |
| 3. | The Safety Directive [1] has addressed all the major topics related to safety, however, the following topics need further consideration:<br>• Management of inspection, maintenance and modification processes,<br>• Proactive learning from experience and benchmarking,<br>• Management of rules and procedures management of commitment, conflict resolution and motivation,<br>• Interface design, work layout and ergonomics,<br>• Maintenance of hardware. | Many railways have developed policies and procedures on these, they can be used as the baseline for developing a common set of procedures compatible with the Safety Directive's objectives and policies. |
| 4. | Harmonisation of SMS through legislation needs centralised support:<br>• To ensure uniform implementation of a common safety policy by different member states,<br>• Create cost-effective and common means to control and monitor the risks. For example, a common EU – wide system for developing and monitoring driver and operator competence and training,<br>• Create a common Incident & Accident reporting and investigation policy for the entire EU railways, with a centralised database for easy access. | A common safety policy, common risk control and monitoring methods, and I&A database have to be developed and agreed among the railways. It is expected that the European Railway Agency will provide the means to achieve these goals. |

| | | |
|---|---|---|
| 5. | Full scale trials of the SMS guidelines [5] should be carried out to check:<br>• if an SMS can be prepared from the available (and accepted by the SA) information;<br>• How much effort and what types of skills are needed to prepare an SMS;<br>• What types of CSTs can be declared in an SMS<br>• Are requirements identified in the SMS guidelines [5] suitable for assessment and certification? Do they provide the basis for auditing? | Full scale trails planned by the Eurotunnel in collaboration with SAMNET could provide some of these answers. Similar trials in other member states would be needed to get the complete information. |
| 6. | The safety method and its dependence on the definition of the railway system, proposed in D2.3.0 [6], needs further investigation. It needs further elaboration and more description at the elemental level. It also has to be acceptable to the majority of stake holders. | Consultation with the stake holders on the Railways System description could be carried out under SAMNET programme. |
| 7. | The accident scenarios and associated hazards types referred in [6] need further investigation. Hazards associated with operations and maintenance need to identified and agreed among the stake holders. Guidelines for calculating risks associated with these hazards are also needed. A consensus is needed on the proposed risk assessment methods. | This could be included in the ERA's programme of work (Activity N$^{o}$ 1). SAMNET can be used to seek consensus on the proposed scenarios, hazards and risk assessment methods. |
| 8. | A consensus is needed on the CSTs and their indexations proposed in D2.4.1 [7]. | SAMNET could be used for this purpose. |
| 9. | Further work is needed to test the proposed risk apportionment scheme based on the AIEF framework (see Sec. 7.7 of D2.4.1 [7]). The AIEF framework needs further development, more detailed description and functional decomposition of AEIF-functions are needed. A consensus on the proposed apportionment scheme is also needed from the stake holders. Some examples of safety targets, e.g. for some specific operations or services, should be constructed, and relationships of these with global safety targets should be explained. | This could be included in the ERA's programme of work (Activity N$^{o}$ 1). SAMNET can be used to seek consensus on this proposal. Safety targets for an inter-state train service are being developed by a SAMNET study group. |
| 10. | The proposed Safety Approval Process (SAP) in D2.5.1 [8] needs more work. It is necessary to specify how part (a) and (b) certification requirements of the safety Directive [1] can be supported by this approach. It should be tried on real systems and services, and refined, and should be supported with detailed guidelines. A | SAMNET can be used to seek consensus on this proposal. |

| | | |
|---|---|---|
| | consensus on the proposed SAP is also needed. | |
| 11. | The "common standard" developed for cross acceptance of POS and ICE3 rolling stocks should be further investigated to check its potential for other systems | SAMNET can explore the possibility of evaluating this standard |
| 12. | On Incident &Accident reporting systems, more work is needed to standardise data collection, analysis and reporting processes in the member states. A consensus on types and categories of I&A events has to be established. The CSIs identified in Annex I of the Safety Directive [1] should be further investigated to establish their exact roles in safety performance measurement. | SAMNET can be used to seek consensus on this proposal. This could be included in the ERA's work programme (Activity N$^{o}$ 3). |
| 13. | A more detailed study should be carried out on the organisational learning to identity how it can be established and supported within an organisation, and at what cost. | This could be included in the ERA's programme of work. |
| 14. | A more concerted effort is required to collect the national safety rules. In order to meet the requirements set out by the Safety Directive, many of the member states are modifying their regulations and safety rules. Guidance is required to ensure that the new national safety rules are not too divergent and burdensome. | This could be included in the ERA's programme of work (Activity N$^{o}$ 4). However, SAMNET can initiate the process by consulting its members and identifying the issues. |
| 15. | Common technical standards should be developed in consultation with the stake holders so that migration to these from national standards could be made easy. | This could be included in the ERA's programme of work (Activity N$^{o}$ 4). |
| 16. | Unification of all operating rules (e.g. rulebooks) is a difficult task, but for specific cross-border operations, a set of common rules can be developed; procedures are needed to perform risk analysis of the rules | This could be included in the ERA's programme of work (Activity N$^{o}$ 4). |
| 17. | A consensus on the proposed Rule Management Framework is needed. A formal mechanism is needed to ensure that activities of all stake holders are properly coordinated in the rule management process. | SAMNET can be used to seek consensus on this proposal. |
| 18. | External resources, such as rolling stock leasing companies and contractors for maintenance and testing work, are used by the railways to provide an efficient and cost effective service. It is important to explain how the Safety Directive [1] should be applied to address the issues related to these topics, for example: | A programme of study to address these topics could be launched by the Commission. |

| | | |
|---|---|---|
| | • whether the scope of RU certification includes organisations operating trains or track maintenance machines operating within possessions.<br>• the certification requirements for rolling stock leasing companies, depots and marshalling yards, and Passenger Transport Authorities who may own rolling stock should be specified. | |
| 19. | The Safety Directive [1] seems to propose a safety approval and acceptance regime based on Certification of RUs and Authorisation of IMs. This, in practice, could be very different to the safety case regime favoured by many Member State (MS) railways. The proposed safety approval regime require further explanation, in particular:<br>• Types and level of detailed evidence needed for certification should be identified.<br>• Conditions for seeking re-approval and recertification should be elaborated, with practical examples. The question of what constitutes a substantial change with regard to the need for re-approval needs further guidance.<br>• The conditions under which SA can revoke the authorisation should be explained. The issue of Conditional Approval is not addressed by the Safety Directive. Depending on extenuating circumstances, a safety authority may have to grant such exemptions. | A programme of study to address these topics could be launched by the Commission. |
| 20. | At present if the infrastructure spans over more than one member state, the safety authorisation task is undertaken by a joint body. From the Safety Directive [1] it is not clear whether in such cases if it will be sufficient for a duty holder to seek authorisation for its SMS from one or other of the member states. | A programme of study to address this topic could be launched by the Commission. |
| 21. | The Safety Directive [1] aims to establish a Transparent and due process, which demands that the following needs are addressed:<br>• A requirement to make applications open for public inspection<br>• Requirements to keep documentation, including audit reports, for set periods.<br>• A right of appeal from a decision to refuse, or to revoke, a safety certificate or authorisation. | A programme of study to address these topics could be launched by the Commission. |

| | | |
|---|---|---|
| 22. | Co-functioning and collaboration between IM and RU are important for the maintaining safety of the overall system. Although the IM is given an important role (Article 9.3), there are no explicit provisions for them to check safety submissions of the RU who seek certificates for approval on their networks. Similarly, the RU should have the opportunity to comment on the safety management system of the IM and of the RU that could affect their operation. | A programme of study to address this topic could be launched by the Commission. |
| 23. | It is not clear what exactly is the jurisdiction of the SA in a given MS when an RU from a different MS does not comply with its certification requirements. | The Commission will require legal expertise to resolve this issue. |
| 24. | New railway standards and procedures are developed or existing standards are modified to implement new safety rules. The Safety Directive [1] should address the requirements for the process of introducing new and revised technical standards. They should ensure that before making these standards mandatory it is proven that they will not undermine safety and will help to achieve the specified safety target levels. | A programme of study to address this topic could be launched by the Commission. |
| 25. | Societal risks are mentioned in the Safety Directive [1] in context of CSTs. There is a lack of consensus among the railways on its definitions, scope and role in safety management. Therefore, a more in depth investigation is needed on this topic and on the acceptance criteria for societal risks. | A programme of study to address this topic could be launched by the Commission. |
| 26. | The requirement for Cost Benefit Analysis (CBA) is identified by the Safety Directive [1] in context of CST proposal. Although CBA is a well known technique used in many fields, its application in determining acceptable risk levels is not widely popular. More work is needed to specify a clear set of criteria for apply CBA. | A programme of study to address this topic could be launched by the Commission. |

# 4 SUGGESTIONS FOR FUTURE WORK

The following topics have been identified for further research:

- **Research on cross cultures issues:**

  The way in which an organisation and its staff behave towards rules is one of the determining factors in the safety culture of the organisation. An open and learning culture should be fostered in Europe which encourages group support for safe behaviour.

- **Development of common standards for cross-acceptance of sub-systems**:

  At present there are a limited set of common safety standards in use in European railways. Unfortunately they mainly address high level signal safety issues, and need further development. The Commission should start a programme of research under which common safety standards for subsystems, such as rolling stocks, signalling equipments, on-board radio equipment, etc. can be developed.

- **Common I&A database for the railways**

  The ERA's work programme Activity N$^{o}$ 3 on safety performance monitoring identifies the requirement for collecting relevant data on safety. However, the existing incident and accident databases of member state railways and that of EuroStat are found to be incompatible to each other in many respects. For example, they use different definitions and their reporting periods are also different. It is advisable that the ERA in collaboration with the stake holders defines and maintains its own database.

- **Integrated organisational learning system for the EU railways**

  Continuous Learning is an integral part of a constantly expanding and changing railway industry. Each member state railways have part formal and part informal processes which have helped them to learn from incidents and accidents and from operational failures of planned processes. They are generally temporary measures not fully supported by management, and therefore often forgotten after the involved parties have moved. The Commission is required to develop an integrated learning system which encompasses all stake holders of EU railways to overcome these problems.

# 5 ABBREVIATIONS AND REFERENCES

## 5.1 Abbreviations

| | |
|---|---|
| CBA | Cost Benefit Analysis |
| CSI | Common Safety Indicator |
| CSM | Common Safety Method |
| CST | Common Safety Target |
| ERA | European Railway Agency |
| I&A | Incident and Accident |
| IM | Infrastructure Manager |
| MS | Member State |
| RU | Railway Undertaking |
| SA | Safety Authority |
| SMS | Safety Management System |

## 5.2 References

1 Directive 2004/49/EC of The European Parliament and of the Council of 29 April 2004 (Railway Safety Directive), Official Journal of the European Union, L164, pp 44-172, 30 April 2004.

2 Regulation (EC) No 1192/2003 modifying No 91/2003 of the European Parliament and of the Council on rail transport statistics.

3 "EN 50126 Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)", 1999.

4 "D.2.1.1: Analysis of Existing Approaches", SAMRAIL/TIFSA/JF/WP2.1/D.2.1.1/V4, October 2003.

5 "Guidelines for Safety Management System", SAMRAIL/SM/D2.2.2/V3.0, May 2004.

6 "D2.3: Common Safety Methods", SAMRAIL/ProRail-SSC/HK-PvdB/WP2.3/V1 D2.3, September 2004.

7 "Acceptable Risk Level", SAMRAIL/DB/PM/WP2.4/V1.0, June 2004.

8 "D2.5.1: Safety Approval and Cross-Acceptance" SAMRAIL/SNCF/JM/WP2.5/D.2.5.1/V02, September 2004.

9 "WP 2.6: Accident and incident reporting system for the EU railways", SAMRAIL/ERRI/GB/WP2.6/D.2.6.1/V2, June 2004.

10 "Organisational Learning from Accidents and Incidents in European Railways" TUDelft/D2.6.0, August 2004.

11 "Position paper on Common Safety Indicators", SAMRAIL/SM/D2.6.1-A, August 2004.

12 "Report D.2.7.1 standards and best practice", SAMRAIL/TÜV-TIT/WP2.7/D2.7.1/V01, June 2004.

13 "Regulations, roles of rules and their unification", SAMRAIL/DTF/LL/WP2.8/D2.8.1-1, June 2004.

14 "SAMNET Glossary", SAMNET/INRETS/ELK/WP0/SAMNET Glossary, April 2003.

15 "Generalised Assessment Method", CASCADE project, 1997.

16 "Deliverable D3: The proposed assessment and certification methodology for digital architectures", ACRuDA project, 1998.