Det Norske Veritas

Final Report – Risk Acceptance Criteria for Technical Systems and Operational Procedures

Report for European Railway Agency
Report No: 24127328/03
Rev: 02

22 January 2010

MANAGING RISK

DNV

Final Report – Risk Acceptance Criteria for Technical Systems and Operational Procedures
for

European Railway Agency
120 rue Marc Lefrancq
59300 Valenciennes
France

DET NORSKE VERITAS LTD.
Highbank House
Exchange Street
Stockport
Cheshire
SK3 0ET
Registered in England
Company No. 1503799

Client ref:	ERA/2009/SAF/S-01	
Report No.:	24127328/03	
Indexing terms:		
Summary:	Final Report to provide an analysis of Risk Acceptance Criteria used in industry. Updated from Rev 0 to address ERA comments. Further minor changes made to address additional comments for Rev 02.	
Prepared by:	*Name and position* Gavin Astin – Principal Consultant Reuben McDonald – Senior Consultant	*Signature* Gavin Astin
Verified by:	*Name and position* John Spouge - Principal Consultant Christoffer Serck-Hanssen – Principal Consultant	*Signature* *Pp* Gavin Astin
Approved by:	*Name and position* Tim Fowler – Transport Team Leader	*Signature* Tim Fowler
Date of issue:	22 January 2010	
Project No:	24127328	

** Please use Project ID as reference in all correspondence with DNV*

Summary of work:

Background

The European Railway Agency (ERA) has let a contract with Det Norske Veritas Limited (DNV), the purpose of which is to research and report on the usage of "Risk Acceptance Criteria for Technical Systems and Operational Procedures".

The objective of this work is to identify the types of Risk Acceptance Criteria (RAC) that are used throughout industry. The ERA also has an interest in learning how acceptance against these RAC is demonstrated. This information may inform ERA's thinking on the use of RAC within the railway sector.

A previously issued Scoping Study identified the following RAC schemes to be taken forward for further consideration:

- The Aviation Industry – European Aviation Safety Agency and the EUROCONTROL Safety Assessment Methodology.
- The Chemical Industry – the Accidental Risk Assessment Methodology (ARAMIS) and modelling system.
- The Great Britain (GB) Rail Industry – the use of RAC within that sector and also the use of the Safety Risk Model.
- The Maritime Industry – the Formal Safety Assessment method as used by the International Maritime Organisation.

This Final Report provides a detailed analysis of each of the schemes listed above.

Findings

Organisations using RAC and their Type

We have identified that harmonised RAC are used in the aviation, nuclear and maritime sectors and also that pan-industry RAC are defined in a number of Member States (see Table 1 and Appendix I for more details).

We note the existence of two options for setting RAC, as follows:

1. "Evidence" based. These are based on historical evidence derived from an analysis of previous safety performance (possibly with an improvement factor built in). These are generally accompanied by substantial reliance on the As Low As Reasonably Practicable (ALARP) and similar concepts to drive safety improvements over time.
2. "Aspirational or technology-driving". These are normally set regardless of whether experience indicates they are currently attainable. Generally RAC that fall into this category place much less reliance on ALARP and similar concepts, and usually achievement of the goal is the end of the matter.

The results of our research indicate that evidence based goals are the norm when setting industry RAC. The exception to this rule applies in The Netherlands, where aspriational RAC are set for industries within that geography.

Derivation and Apportionment of RAC

For the schemes presented above, RAC are usually defined at a high level (representing RAC for the entire operation or undertaking, or possibly at a major hazard level). Where a low level or a *de minimis* criterion is applied (specifically aviation) this has been achieved through an apportionment technique. The apportionment techniques used was based on engineering judgement rather than a rigorous mathematical process.

Demonstrating Compliance with RAC

Bow-tie QRA models are frequently used as the preferred means of assessment. Within these methods human reliability is usually included explicitly.

A number of variants of Safety Integrity Level (SIL) based techniques are used within industry for various purposes, including demonstrating compliance.

We also summarise an approach within ARAMIS that seeks to identify the impact of safety management systems/safety culture and the impact this has on safety performance. This is achieved through an audit process which is then used as an input to the establishment of safety barrier effectiveness.

We have identified no methods or examples that have led to the setting of RAC at the operational level (as would complement the technical system criteria described at Section 3.2). Within the Eurocontrol Safety Assessment Methodology however a process is described to cover the design guidelines for procedures.

Other techniques, such as the use of a risk matrix, provides alternative means of achieving the goals of RAC apportionment and of ensuring that the contribution of individual hazards does not compromise the overall system safety target.

Contents

1.0 Introduction

1.1 Background

The European Railway Agency (ERA) has let a contract with Det Norske Veritas Limited (DNV), the purpose of which is to research and report on the usage of "*Risk Acceptance Criteria for Technical Systems and Operational Procedures*".

The objective of this work is to identify the types of Risk Acceptance Criteria (RAC) that are used throughout industry. The ERA also has an interest in learning how acceptance against these RAC is demonstrated within these industries. This information may inform ERA's thinking on the use of RAC within the railway sector.

DNV's methodology is documented in the project Inception Report [01], and consists of the following two stages:

1. A previously issued Scoping Study [02] to identify and document RAC in use within industry, leading to the selection of four industry sectors (and five RAC schemes) to be taken forward for further consideration. These were:
    a. The Aviation Industry – in particular the European Aviation Safety Agency (EASA) and the EUROCONTROL Safety Assessment Methodology.
    b. The Chemical Industry – in particular the Accidental Risk Assessment Methodology (ARAMIS) risk assessment methodology and modelling system.
    c. The UK Rail Industry – in particular the use of RAC within that sector and also the use of the Safety Risk Model.
    d. The Maritime Industry – in particular the Formal Safety Assessment method as used by the International Maritime Organisation.
2. This Final Report which has the objective of providing a detailed analysis of each of the schemes listed above.

In addition to the areas listed at 1a to 1d above, the Scoping Study considered the use of RAC in the follows area:

- The Aviation Sector as used by the International Civil Aviation Organization.
- The Nuclear Sector at the European Union level through the EURATOM directives.
- The Chemical Sector through the SEVESO directives.
- The Offshore Sector through the International Standards Organisation.
- The Maritime Sector through the International Maritime Organisation.
- The Road Transport Sector through the United Nations Commission for Europe.
- In Great Britain through the Health and Safety Executive (includes analysis of national industry schemes).
- In The Netherlands through the Dutch Ministry.
- In the Norwegian Rail Sector through the Norwegian Railway Administration.

Summary results for each of these sectors and national schemes are provided at Appendix I of this report.

1.2 Limitations

During research for this project it has become clear that the topic of RAC within industry has received a lot of attention, with many 1,000's of documents and research papers published on the subject.

We cannot claim to have read all the literature on this subject, however many of those we have read identify common themes and RAC, matching our own in-house knowledge and expertise.

Whilst our report is an accurate reflection of the information sources and material we have reviewed and confirmed through our own industry experts, it is not possible to claim that our report covers every opinion on the subject.

2.0 Nomenclature and Abbreviations

Term	Description
ADR	Agreement Concerning the International Carriage of Dangerous Goods By Road
ALARA	As Low As Reasonably Achievable
ALARP	As Low As Is Reasonably Practicable
AMC	Acceptable Means of Compliance
ARAMIS	Accidental Risk Assessment Methodology
ARP	Aeronautical Recommended Practice
ATC	Air Traffic Control
ATCO	Air Traffic Control Officer
ATM	Air Traffic Management
ATSU	Air Traffic Services Unit
CAA	Civil Aviation Authority
CBA	Cost Benefit Analysis
CSI	Common Safety Indicator
CSM	Common Safety Method
CST	Common Safety Target
de minimis	A level of risk that is too small to be concerned with
DNV	Det Norske Veritas
EASA	European Aviation Safety Agency
ERA	European Railway Agency
ECAC	European Civil Aviation Conference
ESAM	Eurocontrol Safety Assessment Methodology
ESSAR	Eurocontrol Safety Regulatory Requirement
EURATOM	European Atomic Energy Community
EUROCAE	EURopean Organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration

Term	Description
FHA	Functional Hazard Assessment
FMEA	Failure Modes and Effects Analysis
F-N Curve	A graph showing the frequency F(N) of accidents with N or more fatalities
FSA	Formal Safety Assessment
HEART	Human Error Analysis Reduction Technique
HRA	Human Reliability Analysis
HSW Act	The Health and Safety At Work Act 1974
IAEA	International Atomic Energy Agency
ICAO	International Civil Aviation Organization
IMO	International Maritime Organisation
IRP	Integrated Risk Picture
JAA	Joint Aviation Authority
MAC	Mid Air Collision
MS	European Union Member States
NRV	National Reference Value
PAL	Procedure Assurance Level
PSSA	Preliminary Systems Safety Assessment
RAC	Risk Acceptance Criteria
ROGS	The Railway and Other Guided Transport Systems (Safety) Regulations 2006
SAE	Society of Automobile Engineers
SCW	Safety Critical Work
SESAR	Single European Sky ATM Research
SFAIRP	So Far As Is Reasonably Practicable
SIL	Safety Integrity Level
SMIS	Safety Management Information System
SPAR-H	Standardised Plant Analysis Risk – Human Reliability Analysis
SRM	Safety Risk Model
TLS	Target Level of Safety
ToR	Tolerability of Risk
UN	United Nations

3.0 Background and Context

3.1 Legislative Context

Current European railway legislation, [03], requires that the following should be introduced:

- *'common safety targets (CSTs)' means the safety levels that must at least be reached by different parts of the rail system (such as the conventional rail system, the high speed rail system, long railway tunnels or lines solely used for freight transport) and by the system as a whole, expressed in risk acceptance criteria.*

  The term "*expressed in risk acceptance criteria"* is further defined as "*individual risks relating to passengers, staff including the staff of contractors, level crossing users and others, and, without prejudice to existing national and international liability rules, individual risks relating to unauthorised persons on railway premises*". It also requires "*societal risks*" to be addressed, although does not specify any specific measures.

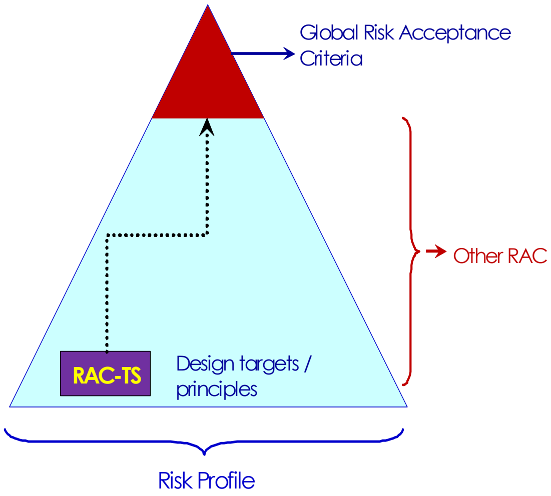
- *'common safety methods (CSMs)' means the methods to be developed to describe how safety levels and achievement of safety targets and compliance with other safety requirements are assessed.*

Finally, in order to facilitate the monitoring of the CSTs the directive also requires the use of Common Safety Indicators, CSIs. The purpose of the indicators is to:

- "*facilitate the assessment of the achievement of the CST and to provide for the monitoring of the general development of railway safety*".

A first set of CSTs was adopted in early 2009. In addition, an equivalent set of National Reference Values (NRV) were derived for each Member State.

3.2 Current Status



ERA's current thinking is described with reference to the hierarchy of available RAC (shown opposite).

At the "global" or high level, RAC may be defined in generic terms for the entirety of a railway undertaking (e.g. the system as a whole). An advantage of this approach is that it allows each railway undertaking to choose between one of many ways to mitigate the total risk. A disadvantage however is that the risk controls put in place by one railway undertaking may not be in place in another. This limits the ability for harmonisation and cross-acceptance.

Conversely RAC could be specified at a "technical" level (possibly functional level, hazard level, procedural level or equipment level), thus relying more on the inherent safety of the individual equipments and/or processes. Whilst this has the disadvantage of removing some of the flexibility described above, it does have advantages. For example, if a *de minimis* safety indicator were specified at a low level it may be possible to use this as a basis for cross-acceptance across Member States. In this respect the ERA has indicated [04] they are considering the use of a low level criterion for technical systems (and potentially operational processes).

A *de minimis* criterion has already been defined, for technical systems only, by the ERA as follows:

> *Where hazards arise from failures of technical systems … the following risk acceptance criterion shall apply for the design of technical system:*
>
> *For technical systems where a functional failure has a credible direct potential for a catastrophic consequence, the associated risk does not have to be reduced further if the rate of that failure is less than or equal to 10^{-9} per operating hour.*
>
> *Nevertheless, if the proposer can demonstrate that the national safety level can be maintained with a less demanding criterion than the 10^{-9}, this criterion can be used by the proposer.*

3.3 Commentary and Objectives

The definition of CSTs is not prescriptive about how RAC are to be derived or whether a formal link should exist between whole system level RAC and other related criteria which may be specified at lower levels of system indenture.

We also note the inclusion of a *de minimis* target (for technical systems) and of the allocation of NRVs (Section 3.2). The objective of such criterion being to maintain national safety performance levels amongst Member States.

Considering this the objectives of this Final Report are to study identified industry sector uses of RAC and for each to address ERA's objectives that "*for each sector, the RAC should be identified at a technical level,* [and] *also at an operational/procedural level. These could be either:*

- *Quantitative in forms of tolerable hazard rates or human reliability;*
- *Semi-quantitative as Safety Integrity Levels…;*
- *Qualitative as rules to accept human driven actions;*
- *In any other form that allows assessment and acceptance of the systems."*

Also, the minimum requirements for performing safety critical tasks should be analysed by studying either relevant legislation, guidance or safety management systems. These may also range from quantitative values for the human reliability to description of principles on education or redundancy through check by different people.

4.0 Scoping Report and Objectives of this Final Report

4.1 Summary of Research Completed (Scoping Report)

As a precursor to this report DNV completed a Scoping Study, [02], making the following general observations about the structure of RAC:

1. At the international level (e.g. United Nations) it is unusual for harmonised RAC to be specified (although exceptions exist such as the International Civil Aviation Organization and the International Maritime Organisation).
2. At a regional level (Europe for this study) it is more common for harmonised RAC to be specified. For example the European Aviation Safety Agency, Eurocontrol and the European Atomic Energy Community specify RAC. Other industries, for example the chemical sector through the European Seveso Directives, require certain sites to develop a safety report (which require risk based arguments to be presented, although specific RAC are not stated).
3. At national level it is usual for RAC to be specified or for alternative prescriptive requirements for risk and safety management to be identified.
4. Within each country it is common for company and/or industry safety risk schemes (containing RAC) to exist. These schemes are structured to meet national/regional and international regulations as well as company goals and objectives.

We also observed that RAC defined at levels 1 and 2 tend to be at a high or catastrophic hazard level, for example a mid-air collision for aviation, or an annual risk of fatality for crew members, passengers/public in the maritime sector.

At a national level, RAC are typically specified as an individual risk of fatality for workers/members of the public. National level RAC are not usually industry specific. Additionally societal risk criteria may also be specified.

RAC are usually specified in most detail at company level and within national industry safety schemes. At this level it is more common for RAC to be apportioned to business activities or sub-hazards (see Table 30).

We note that for most of the schemes studied, RAC are derived based on past performance. We have referred to these as evidence based RAC. RAC derived in The Netherlands provide an exception to this rule. Here, technology driving / aspriorational RAC are set. Such RAC are specified regardless of whether history suggests they can be attained.

We provide a summary, from our Scoping Report, of the use of RAC in industry in the table below. More details are included at Appendix I of this report.

Table 1: Summary of Application of RAC in Industry[1]

	RAC Hierarchy	RAC Form	RAC Type	Standardised Calculation Tools	Comments
Aviation (all)	Major hazard level	Target safety level / tolerable hazard rate	Quantitative	Standard tools are provided	
Nuclear	Permitted consequence (dosage) levels to an individual over a stated period of time		Quantitative	Standard dosage calculation methods are provided	This sector uses human error prediction techniques extensively.
Chemical	None	None	None	Yes	A risk assessment method has been created through a European Research project. The methodology includes safety culture and human error assessment processes
International Offshore	None	None	None	No	The offshore regulations are goal based and no RAC are defined. National regulations apply relating to risk assessment processes
Maritime – FSA	High level	Individual and societal risk	Quantitative	No	
Maritime – High Speed Craft	Major hazard level	Tolerable hazard rate	Quantitative	No	There is a requirement within this system that any failure mode that can lead to a catastrophic consequence must be mitigated by redundancy if it cannot be shown to be "extremely improbable"
Dangerous Goods by Road	None	None	None	None	Contains qualitative statements that risk must be managed. The Organisation for Economic Co-operation and Development (OECD) and the World Road Association (PIARC) have jointly developed a quantitative risk assessment model (DG-QRAM) to evaluate the risks of dangerous goods transport through road tunnels.
UK Rail	High level	Expressed in terms fatalities/injuries per passenger kilometre (or hour worked)	Quantitative	Standard tools are provided	
UK Offshore	High level	Individual risk	Quantitative	None	HSE guidance is provided
Company Scheme	High level	Societal risk	Quantitative via F-N curve.	Standard tools are provided	

[1] See Section 5.0 and Appendix I for more details

5.0 Our Findings

5.1 European Aviation Safety Agency: Aircraft Design

5.1.1 What is it and what is it used for?

Aircraft design is an international endeavour with large passenger aircraft only being developed by a small number of manufacturers. Aircraft are evidently international vehicles and will travel between countries and continents, therefore the certification of on civil airborne systems and equipment has been aligned internationally for some time.

In Europe, the Joint Aviation Authorities (JAA) developed risk acceptance criteria and guidance on their application, the JAA has now been succeeded for the purpose of European aviation rulemaking by the EASA continuing effectively the same approach. A very similar approach is used in the United States by the Federal Aviation Administration (FAA). The scheme used is highly analogous to the scheme used to analyse high-speed craft as described in Table 22.

The risk target is that a **catastrophic failure should not occur more often than 1.0 x 10^{-9} per flight hour.** Other targets have been specified for Hazardous, Major and Minor severity effects and are summarised below in **Figure 1**.

In addition to this risk criterion, a fail-safe design concept is applied, this states:

1. In any system or subsystem, the failure of any single element, component, or connection during any one flight should….regardless of its probability…not be Catastrophic.
2. Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be assumed, unless their joint probability with the first failure is shown to be extremely improbable.

5.1.2 Derivation of risk criteria

The derivation of this high level target has been detailed in JAR AMJ 25.1309 and [06]:

- Historical evidence indicates a risk of serious accident due to operational and airframe related causes of approximately 1 per million flights (10^{-6} per flight hour)
- It seems reasonable that serious accidents caused by systems should not be allowed a higher probability than this in new aeroplane designs
- 10% of this risk is allocated to an aircraft system failure (10^{-7} per flight hour)
- For this reason it is assumed, arbitrarily, that there are about 100 potential failure conditions in an aeroplane which would prevent continued safe flight and landing. This leads to a maximum permissible frequency of 10^{-9} per flight hour per catastrophic failure condition
- Lesser severities are allowed with probabilities up to 2 orders of magnitude higher as shown in the table below

The derivation is therefore initially based on historical accident risk, but then makes considerable assumptions regarding how this relates to aircraft systems, and gives them all the same weighting. The apportionment into 100 failure modes was based on engineering judgement rather than a mapping of aircraft systems.

The quantitative probability is expressed in terms of flight hours, no further allowance or sub-categorisation is made for specific phases of flight.

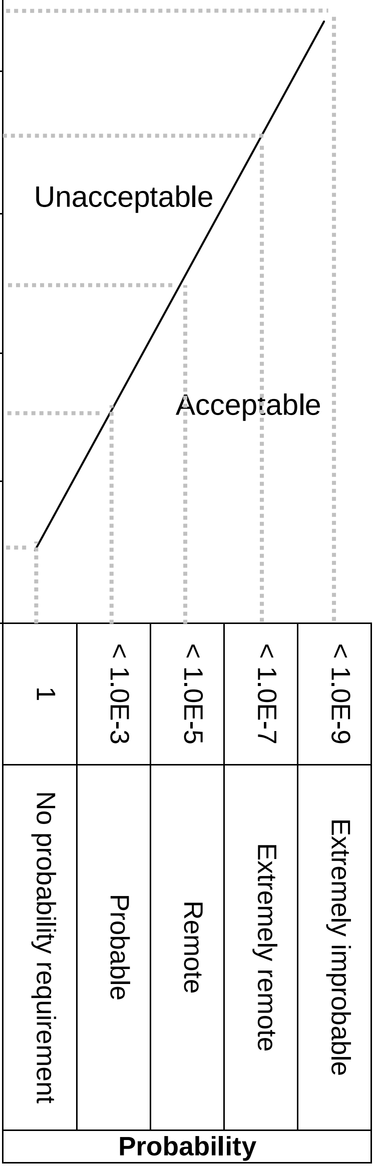
Severities are given a classification of catastrophic, hazardous, major etc and to aid interpretation of these expressed qualitatively in terms of three parameterisations:

- Effect on aeroplane
- Effect on occupants
- Effect on flight crew

If is not technologically or economically practicable to meet the numerical criteria for a catastrophic failure condition, the safety objective may be met by accomplishing all of the following:

1. Utilising well proven methods for the design and construction of the system; and
2. Determining the average probability per flight hour of each failure condition using structured methods, such as Fault Tree Analysis, Markov Analysis, or Dependency Diagrams; and
3. Demonstrating that the sum of the average probabilities per flight hour of all catastrophic failure conditions caused by systems is of the order of 10^{-7} or less.

Severity			
Effect on Flight Crew	**Effect on Occupants**	**Effect on Aeroplane**	**Severity Class**
Fatalities or incapacitation	Multiple Fatalities	Normally with hull loss	Catastrophic
Physical distress or excessive workload impairs ability to perform tasks	Serious or fatal injury to a small number of passengers or cabin crew	Large reduction in functional capabilities or safety margins	Hazardous
Physical discomfort or a significant increase in workload	Physical distress possibly including injuries	Significant reduction in functional capabilities or safety margins	Major
Slight increase in workload	Physical discomfort	Slight reduction in functional capabilities or safety margins	Minor
No effect	Inconvenience	No effect on operational capabilities or safefy	No safety effect



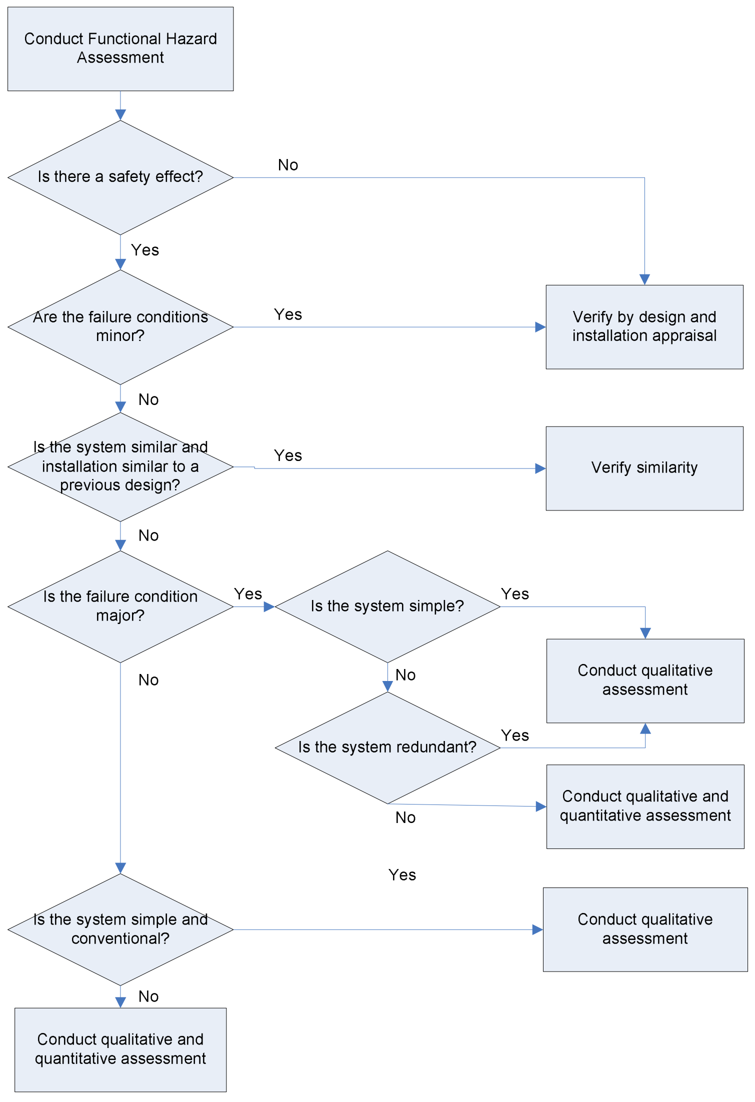
Stage 1: Determine the highest severity for a given event, be that the impact on flight crew, occupants or the aircraft.

Stage 2: This then becomes the Severity Class, the graph can then be read across to determine the maximum acceptable probability for that event.

Figure 1: EASA Risk Classification Scheme for Aircraft Design

5.1.3 What it includes

Guidelines and methods for conducting safety assessments on civil airborne systems and equipment are detailed by EASA in their Certification Specifications, CS-25 and further elaborated by the Society of Automotive Engineers (SAE) are presented in Aeronautical Recommended Practises (ARP) 4761. EASA specifications define the following process shown in Figure 2.


Conduct Functional Hazard Assessment
Is there a safety effect?
No
Yes
Are the failure conditions minor?
Yes
Verify by design and installation appraisal
No
Is the system similar and installation similar to a previous design?
Yes
Verify similarity
No
Is the failure condition major?
Yes
Is the system simple?
Yes
Conduct qualitative assessment
No
No
Is the system redundant?
Yes
Conduct qualitative and quantitative assessment
No
Yes
Is the system simple and conventional?
Conduct qualitative assessment
No
Conduct qualitative and quantitative assessment

A Functional Hazard Assessment (FHA) is conducted at the beginning of the aircraft/system development cycle.

FHA is a systematic, comprehensive examination of aeroplane and system functions to identify potential minor, major, hazardous, and catastrophic failure conditions which may arise, not only as a result of malfunctions or failure to function, but also as a result of normal responses to unusual or abnormal external factors.

This FHA assessment may be conducted using service experience, engineering and operational judgement, and/or a top-down deductive qualitative examination of each function.

Figure 2: Depth of Analysis Flowchart from EASA [06]

An assessment to identify and classify failure conditions is necessarily qualitative. On the other hand, an assessment of the probability of a failure condition may be either qualitative or quantitative. An analysis may range from a simple report that interprets test results or compares two similar systems to a detailed analysis that may or may not include estimated numerical probabilities. The depth and scope of an analysis depends on the types of functions performed by the system, the severity of failure conditions, and whether or not the system is complex.

Various methods for assessing the causes, severity, and probability of failure conditions are available to support experienced engineering and operational judgement after the FHA. Some of these methods are structured. The various types of analysis are based on either inductive or deductive approaches. Probability assessments may be qualitative or quantitative.

Edited descriptions of some types of analysis recommended in [06] are provided below, full details are available in ARP 4761 [07]:

- *Design Appraisal.* This is a qualitative appraisal of the integrity and safety of the system design.
- *Installation Appraisal.* This is a qualitative appraisal of the integrity and safety of the installation. Any deviations from normal, industry accepted installation practices, such as clearances or tolerances, should be evaluated, especially when appraising modifications made after entry into service.
- *Failure Modes and Effects Analysis.* This is a structured, inductive, bottom-up analysis, which is used to evaluate the effects on the system and the aeroplane of each possible element or component failure. When properly formatted, it will aid in identifying latent failures and the possible causes of each failure mode. The ARP 4761 [07] provides methodology and detailed guidelines, which may be used to perform this type of analysis.
- *Fault Tree or Dependence Diagram Analysis.* Structured, deductive, top-down analyses that are used to identify the conditions, failures, and events that would cause each defined failure condition. A failure modes and effects analysis may be used as the source document for those primary failures or other events.
- *Markov Analysis.* A Markov model (chain) represents various system states and the relationships among them. The states can be either operational or non-*operational*. The transitions from one state to another are a function of the failure and repair rates. Markov analysis can be used as a replacement for fault tree/dependence diagram analysis, but it often leads to more complex representation, especially when the system has many states.
- *Common Cause Analysis.* The acceptance of adequate probability of failure conditions is often derived from the assessment of multiple systems based on the *assumption* that failures are independent. Therefore, it is necessary to recognise that such independence may not exist in the practical sense and specific studies are necessary to ensure that independence can either be assured or deemed acceptable.

The Common Cause Analysis is sub-divided into three areas of study:

1. *Zonal Safety Analysis.* This analysis has the objective of ensuring that the equipment installations within each zone of the aeroplane are at an adequate safety standard with respect to design and installation standards, interference between systems, and maintenance errors.
2. *Particular Risk Analysis.* Particular risks are defined as those events or influences, which are outside the systems concerned. Examples are fire, leaking fluids, bird strike, tyre burst, high intensity radiated fields exposure, lightning, uncontained failure of high energy rotating machines, etc. Each risk should be the subject of a specific study to examine and document the simultaneous or cascading effects or influences, which may violate independence.
3. *Common Mode Analysis.* This analysis is performed to confirm the assumed independence of the events, which were considered in combination for a given failure condition.

5.1.4 What is excluded

The EASA risk criteria and assessment methodology refer to aircraft systems. Human factors are not specifically included although they are elsewhere, in [06] for example.

5.1.5 Summary and Comparison with ERA's Study Objectives

The study objectives are stated in Section 3.3:

1. *The identification of RAC at a technical level and operational/procedural level.*

RAC are specified at a technical level for aircraft systems, with a relationship back to an apportioned historical accident risk. An assumption is made that there are 100 potential failure modes that can contribute to this historic risk and an apportionment is made equally between these. This is a low level criteria specified per system against a catastrophic accident. Additional criteria are specified for major, minor etc. categories.

2. *Are human reliability or semi quantitative techniques such as the SILs or other qualitative rules used to accept human driven actions that allow assessment and acceptance of the systems?*

The EASA methodology has a scope that only includes the aircraft systems, a significant amount of the total aviation risk budget (>80%) is remaining once Air Traffic Management and Aircraft Design are excluded for the historical accident rate and this would be likely to be taken up by pilot error, however this is outside the scope of this methodology.

3. *The minimum requirements for performing safety critical tasks should be analysed by studying relevant legislation, guidance or safety management systems. These may also range from quantitative values for the human reliability to description of principles on education or redundancy through check by different people.*

As above, human tasks are outside the scope of the EASA criteria.

We conclude by asking ***could the EASA (or similar) be used in the context of assigning RAC?*** The answer to this question is yes, because for specific equipment certification requirements the methodology and criteria work well, and have been globally accepted for a considerable amount of time. However the scope for the EASA criteria is limited to the design of a safe aircraft, and other factors including human performance and considered in complementary safety assessments such as the EUROCONTROL SAM, or considered to be covered by pilot training requirements.

5.2 ESARR 4 Design Target and the EUROCONTROL SAM

5.2.1 ESARR 4 Design Target

5.2.1.1 What is it and what is it used for?

The ESARR 4 Design Target is a high Level risk target applicable to the Air Traffic Management (ATM) contribution to aviation accidents; this is a relatively small contribution to all aviation risk, accounting for approximately 2% of aircraft accidents.

The target states that:

The maximum tolerable probability of ATM directly contributing to an accident of a Commercial Air Transport aircraft of 1.55x10^{-8} accidents per flight hour.

The target was first published as part of the EUROCONTROL Safety And Regulatory Requirements (ESARR), as part of ESARR 4: Risk Assessment and Mitigation in ATM. ESARR4 came into force in April 2004. All 44 European Civil Aviation Conference (ECAC) states should be using it in risk assessment of new or changed ATM systems. Commercial Air Transport Aircraft refer to passenger and cargo services and non-revenue services of those aircraft.

It has since been included as part of the EU common requirements laying down common requirements for the provision of air navigation services CR 2096/2005.

5.2.1.2 How was it derived?

The process, together with related justifications and assumptions, documented in EUROCONTROL Safety Regulatory Commission (SRC) Policy Doc. 1 are as follows:

- ICAO ADREP database was reviewed for the period 1988 to 1999 in the ECAC region.
- Over this 12-year period 374 accidents have been registered.
- This leads to an average of 31.17 accidents per year.
- Based on a report from the UK Civil Aviation Authority (CAA), it was derived that the percentage of fatal accidents with at least one Air Traffic Control (ATC) primary cause - i.e. ATC directly causing the accident - was 1.1%.
- Since ATM encompasses several functions, as well as ATC, the maximum direct ATM contribution to the total number of accidents was assumed to be 2%. Consequently this led to a value of 0.623 accidents per year with a 'direct' ATM contribution.
- With the 1999 traffic volume in the ECAC area, the 0.623 figure led to an ECAC safety minimum of 4.38 x 10^{-8} accidents per flight hour.
- Then a 6.7% traffic increase per annum was assumed which led to a number of flight hours by 2015 of 4.01 x 10^{7}.
- With the ATM 2000+ objective that the number of ATM induced accidents and serious or risk bearing incidents shall at least not increase, the 0.623 accidents per year was applied as well in 2015 and 0.623/4.01 x 10^{+7} leads to 1.55 x 10^{-8} accidents per flight hour with a direct ATM contribution or 2.31 x 10^{-8} accidents per flight assuming a 1.5 hr average flight duration.

This can be summarised in Figure 3 below.

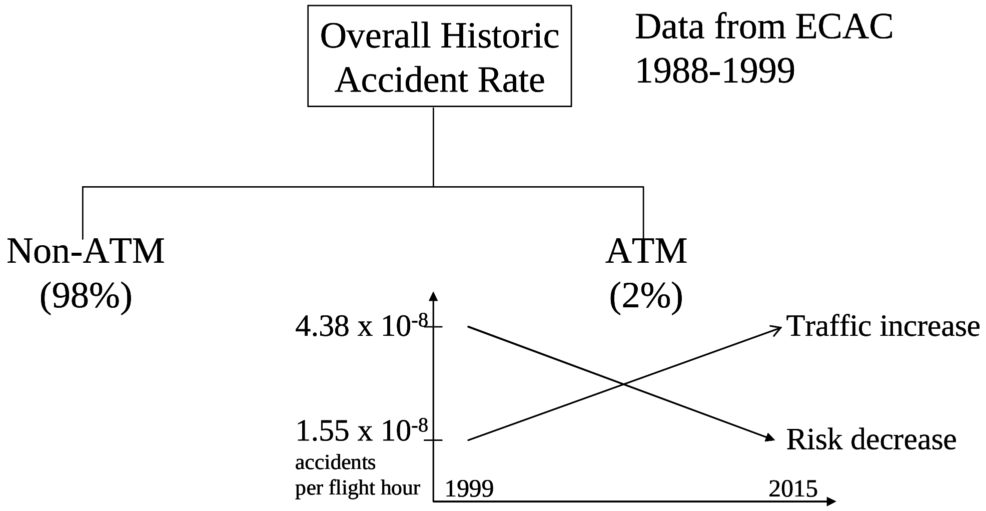
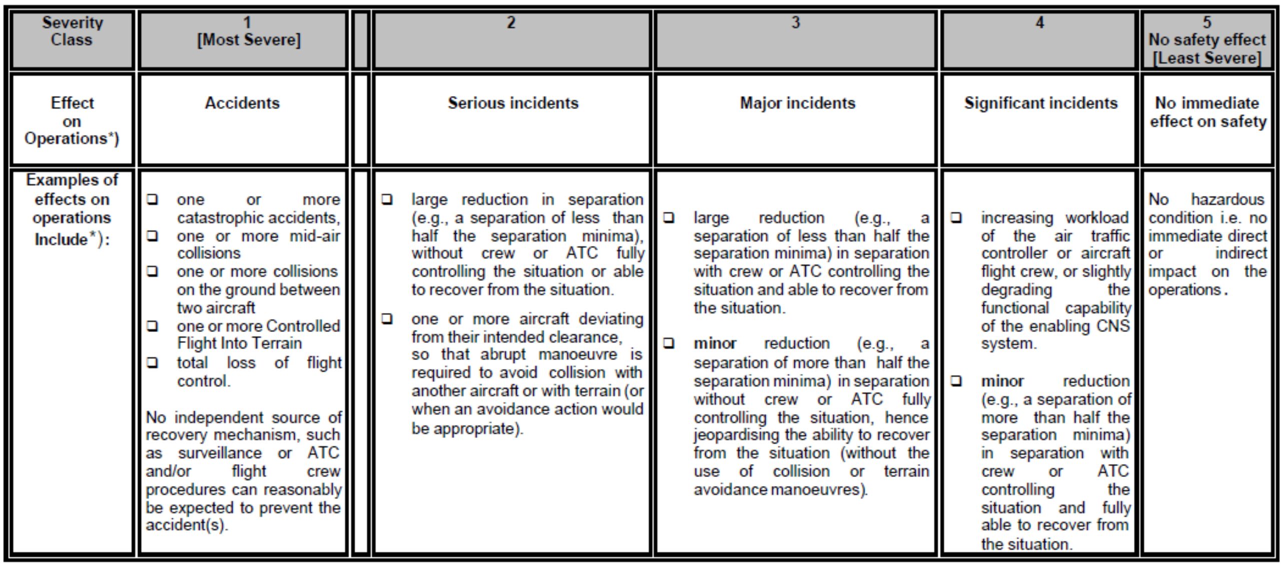


Figure 3: Summary of Derivation of the ESARR 4 Risk Criteria

ESARR 4 includes a severity classification scheme which allows the classification of accidents, serious incidents, major incidents, significant incidents. This is shown below in Table 2.

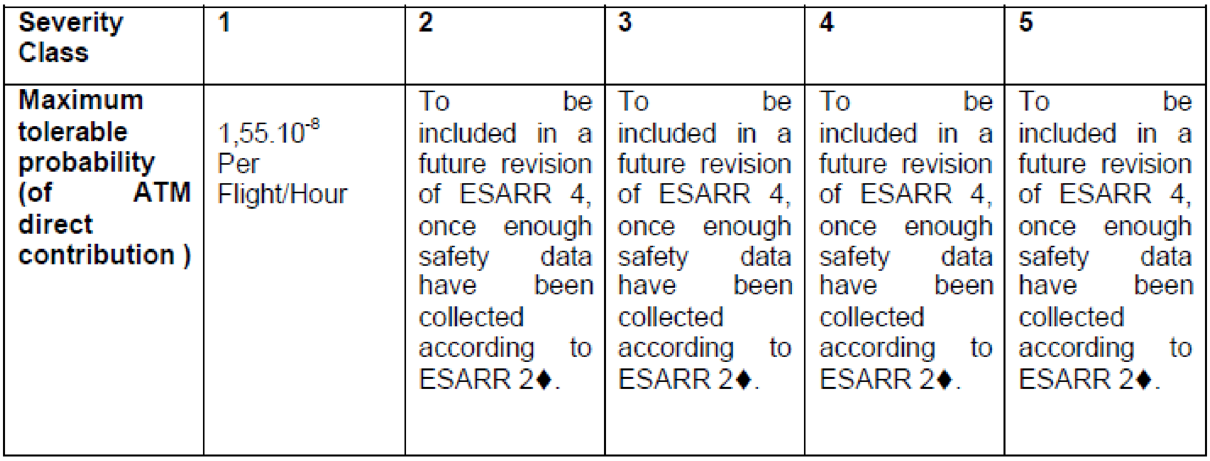
The risk classification scheme including the accident frequency value is shown in Table 3, in ESARR 4, a frequency target for severity category 1 (accidents) is given but not for the other accident severities. Eurocontrol is currently reviewing and determining tolerable probabilities for these other severities, but no accepted value has been published.

Table 2: ESARR 4 Severity Classification Scheme



Severity Class	1 [Most Severe]		2	3	4	5 No safety effect [Least Severe]
Effect on Operations*)	Accidents		Serious incidents	Major incidents	Significant incidents	No immediate effect on safety
Examples of effects on operations Include*):	❑ one or more catastrophic accidents, ❑ one or more mid-air collisions ❑ one or more collisions on the ground between two aircraft ❑ one or more Controlled Flight Into Terrain ❑ total loss of flight control. No independent source of recovery mechanism, such as surveillance or ATC and/or flight crew procedures can reasonably be expected to prevent the accident(s).		❑ large reduction in separation (e.g., a separation of less than half the separation minima), without crew or ATC fully controlling the situation or able to recover from the situation. ❑ one or more aircraft deviating from their intended clearance, so that abrupt manoeuvre is required to avoid collision with another aircraft or with terrain (or when an avoidance action would be appropriate).	❑ large reduction (e.g., a separation of less than half the separation minima) in separation with crew or ATC controlling the situation and able to recover from the situation. ❑ **minor** reduction (e.g., a separation of more than half the separation minima) in separation without crew or ATC fully controlling the situation, hence jeopardising the ability to recover from the situation (without the use of collision or terrain avoidance manoeuvres).	❑ increasing workload of the air traffic controller or aircraft flight crew, or slightly degrading the functional capability of the enabling CNS system. ❑ **minor** reduction (e.g., a separation of more than half the separation minima) in separation with crew or ATC controlling the situation and fully able to recover from the situation.	No hazardous condition i.e. no immediate direct or indirect impact on the operations.

Table 3: ESARR 4 Risk classification scheme



Severity Class	**1**	**2**	**3**	**4**	**5**
Maximum tolerable probability (of ATM direct contribution)	$1,55.10^{-8}$ Per Flight/Hour	To be included in a future revision of ESARR 4, once enough safety data have been collected according to ESARR 2♦.	To be included in a future revision of ESARR 4, once enough safety data have been collected according to ESARR 2♦.	To be included in a future revision of ESARR 4, once enough safety data have been collected according to ESARR 2♦.	To be included in a future revision of ESARR 4, once enough safety data have been collected according to ESARR 2♦.

Since the publication of the ESARR 4 document, there has not been a formal update and there is no scheduled date for an update. However some effort to update the figures used has been made. One effort led by the European Organisation for Civil Aviation Equipment (Eurocae) has resulted in the drafting of the guidance document entitled ED-125: Process for Specifying Risk Classification Scheme and Deriving Safety Objectives in ATM “in compliance” with ESARR 4 [32].

5.2.1.3 Eurocae ED-125

Eurocae Working Group 64 on Air Traffic Management Risk Assessment developed the Eurocae ED-125 [32] document. This provides additional information for constructing a risk classification scheme which is in compliance with ESARR 4. This is however a guidance document rather than a required standard.

The ED-125 document specifies “Safety Targets”. These define the overall maximum frequency of occurrence of effects of any type having a given Severity Class, whatever the ATM cause. It also provides some justification of these safety targets for lower severity events.

ED-125 proposes the following National Regulatory Safety Targets:

Safety Target 1 (severity class 1)	1E-08 per flight hour
Safety Target 2 (severity class 2)	1E-05 per flight hour
Safety Target 3 (severity class 3)	1E-04 per flight hour
Safety Target 4 (severity class 4)	1E-02 per flight hour

The derivation of these numbers has also been explained in the ED-125 document. **Safety Target 1** is set to the same order of magnitude as ESARR4 Safety Target for the catastrophic severity class. The Eurocae Working Group decided to keep the same order of magnitude as the ESARR4 value which has been recently published and enforced.

Safety Target 2 was derived from data collected by various air traffic management service providers on the number of serious incidents that had been recorded in their airspace. The data were collected in various geographical and complexity areas and airspace types. The analysis of collected data showed that the number of Serious Incidents were on an average in the order of magnitude of one per 100,000 flight-hours. Thus WG64 decided to keep this value as the Regulatory Safety Target.

Safety Target 3 and 4 were not derived purely from data due to the limits of recording such low severity events. **Safety Target 3** was set in the order of magnitude of one per 10,000 flight-hours using a mix of data analysis of Major Incidents and operational tolerability. **Safety Target 4** was set in the order of magnitude of one per 100 flight-hours they were determined using operational tolerability. Operational judgment on the tolerability of the number of such occurrences per year was set from an organisation point of view as well as the tolerability of the total number of such occurrences per Air Traffic Control Officer (ATCO) career duration.

5.2.1.4 Usage

ESARR4 and CR2096/2005 specify that the design target should be used within a risk management framework. This shall include hazard identification as well as risk assessment and mitigation and it is required that any changes to the ATM System and supporting services are subject to assessment which addresses:

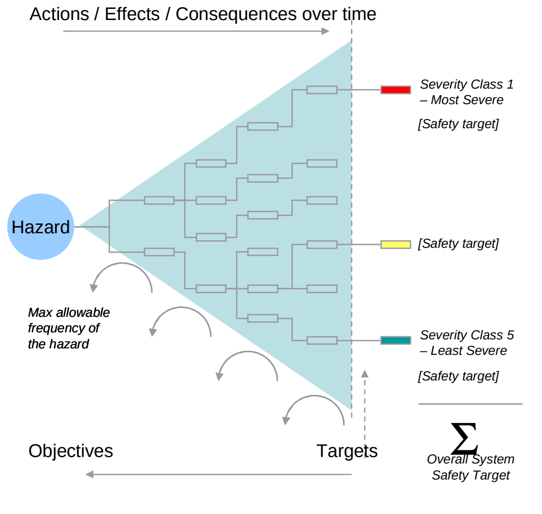
- The complete life-cycle of the constituent part of the ATM System under consideration, from initial planning and definition to post-implementation operations, maintenance and de-commissioning;
- The airborne and ground components of the ATM System, through cooperation with responsible parties; and
- The three different types of ATM elements (human, procedures and equipment), the interactions between these elements and the interactions between the constituent part under consideration and the remainder of the ATM System.

A high-level description is provided below that describes this risk assessment methodology. In practice each European state has developed separate risk assessment methodologies that should be compatible with the ESARR 4 requirements. These frameworks can appear to be very different, e.g. some are risk matrix based, whilst some require quantitative calculations to be made.

Certain methodologies have been formally assessed by Eurocontrol in their compliance with the ESARR 4 requirements [08]; these include the Eurocontrol Safety Assessment Methodology (E-SAM), the EUROCAE ED78A methodology and the other safety criteria. In the rest of this section, the Eurocontrol SAM shall be studied in greater detail and its requirements meeting the ESARR 4 Risk Target.

5.2.2 EUROCONTROL Safety Assessment Methodology

The Eurocontrol Safety Assessment methodology is a complex methodology but can be summarised as a three stage process, a FHA, Preliminary Systems Safety Assessment (PSSA) and a Systems Safety Assessment (SSA).

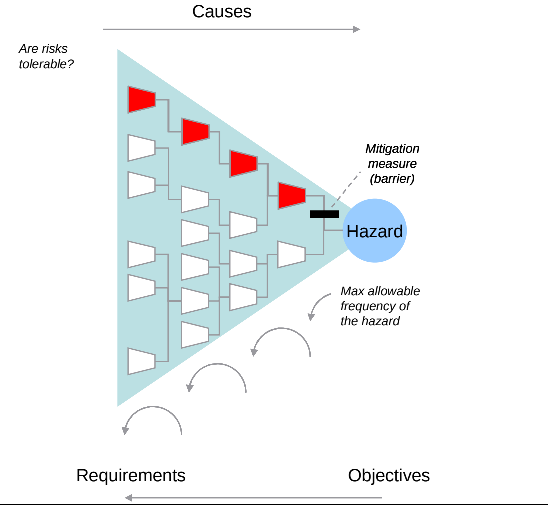

Actions / Effects / Consequences over time
Severity Class 1 – Most Severe
[Safety target]
Hazard
[Safety target]
Max allowable frequency of the hazard
Severity Class 5 – Least Severe
[Safety target]
Objectives
Targets
∑
Overall System Safety Target

Functional Hazard Assessment (FHA)

In the FHA, hazards relating to the system are identified, from these hazards possible severities are determined, with a severity class matching those specified in Table 2.

An apportioned factor of the ESARR 4 requirement would then be used against the severity class 1 events, this is called the *safety target*, this can then be back-calculated to determine the maximum allowable frequency of that hazard. This is the so called *safety objective*.

Between these, various mitigations exist that reduce the likelihood that the hazard will lead to a severity class 1 event. Certain mitigations called “safety nets” that exist in reality are often excluded as a barrier from this analysis on the basis that the system should be acceptably safe without them, and they provide an additional level of safety. These include the Airborne Collision Avoidance System (ACAS) and the Terrain Awareness and Warning System (TAWS).

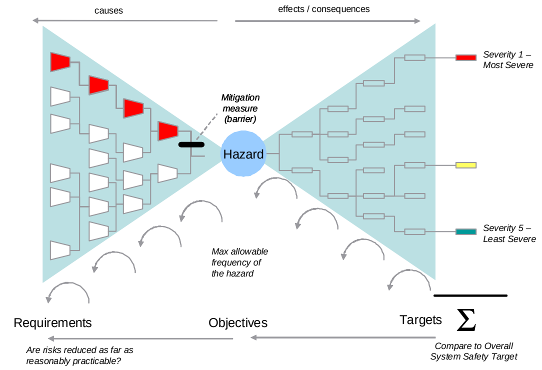

Causes
Are risks tolerable?
Mitigation measure (barrier)
Hazard
Max allowable frequency of the hazard
Requirements
Objectives

Preliminary Systems Safety Assessment (PSSA)

In the PSSA safety objectives developed in the FHA are then used to set safety requirements for each part of the system.

Suitable risk mitigation measures (barriers) should be identified if the system does not meet the required safety targets OR risks are not reduced as far as reasonably practical.

This is still done at the pre-operational level and hence is termed “Preliminary”.


causes
effects / consequences
Severity 1 – Most Severe
Mitigation measure (barrier)
Hazard
Severity 5 – Least Severe
Max allowable frequency of the hazard
Requirements
Objectives
Targets
∑
Are risks reduced as far as reasonably practicable?
Compare to Overall System Safety Target

Systems Safety Assessment (SSA)

The system safety assessment is performed and covers many different activities including:

- System element design and implementations
- Design development and implementation processes
- Verification and validation of processes and results (inc. testing)
- Competency of personnel undertaking and managing all aspects of the work
- Collection and analysis of data (metrics) concerning both the product and the process

Figure 4: Outline of the Eurocontrol Safety assessment Methodology

Although represented relatively simply above, the E-SAM includes a large toolbox of techniques and information with SAM Electronic including 91 documents of techniques and guidance [09]. The sections most relevant to the project are the apportionment of the high-level ESARR 4 target and how procedures / human factors are managed.

5.2.2.1 Apportionment of high-level targets

The Eurocontrol SAM methodology allows several methods to be used for apportioning the high level system target to the sub-system level.

There are actually two types of apportionment; the first is from the overall high-level target down to a target for the system under investigation. The second is the apportionment of the system level target between the various hazards under investigation.

The first apportionment is often complex and shall be considered in more detail below. There are several methods used to apportion a high level risk target. It can be broken down absolutely as shown below in Figure 5, this is the most difficult and most prone to error. Some guidance has been provided on this apportionment primarily around different flight phases, however there is no guarantee that the portion of the overall risk budget taken for the sub-system under consideration is accurate compared with historical experience or compared with the budget taken for other sub-systems.

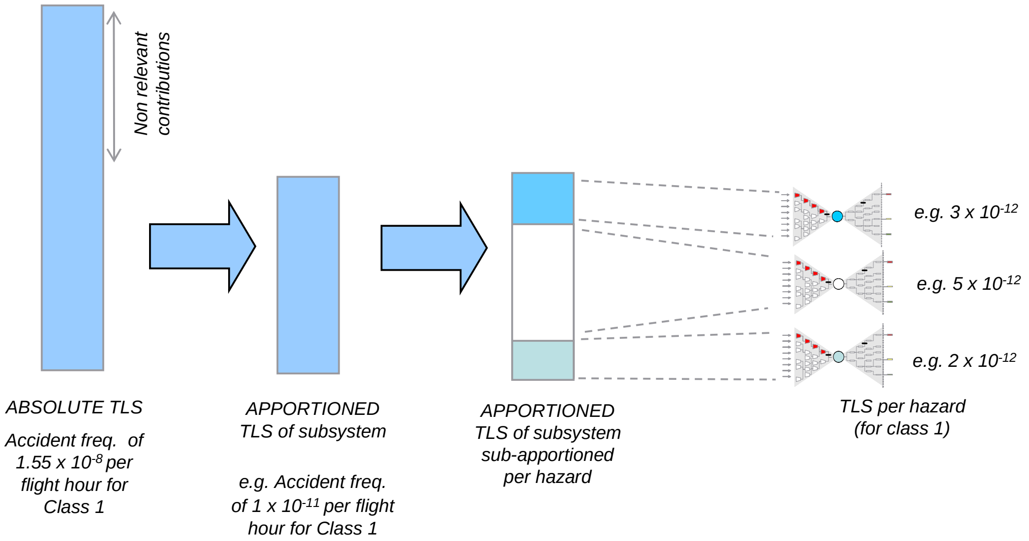

Non relevant contributions
e.g. 3 x 10^{-12}
e.g. 5 x 10^{-12}
e.g. 2 x 10^{-12}
ABSOLUTE TLS
Accident freq. of 1.55 x 10^{-8} per flight hour for Class 1
APPORTIONED TLS of subsystem
e.g. Accident freq. of 1 x 10^{-11} per flight hour for Class 1
APPORTIONED TLS of subsystem sub-apportioned per hazard
TLS per hazard (for class 1)

Figure 5: Direct apportionment of a high level TLS

In recent years a more consistent approach has been developed in the form of the Integrated Risk Picture (IRP), this is a risk model that has been developed by EUROCONTROL by reviewing accident and incident data and encompassing the entire ATM system. The IRP therefore allows sub-system apportionment in a consistent manner based on the historical performance of those systems and ensures that the high level target is considered in a holistic manner.

The IRP has also been used in the past to determine which parts of the system are most critical to safety performance, and where additional effort should be concentrated.

In Figure 7 below a consistent apportionment is represented guided by the output from the IRP model.

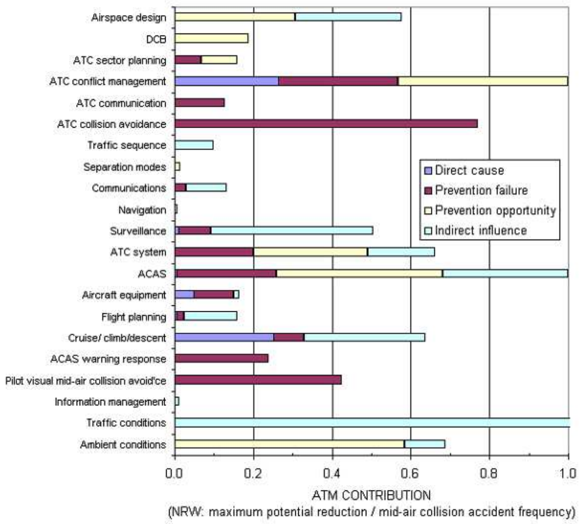


Figure 6: Output results from the IRP regarding the impact of different systems

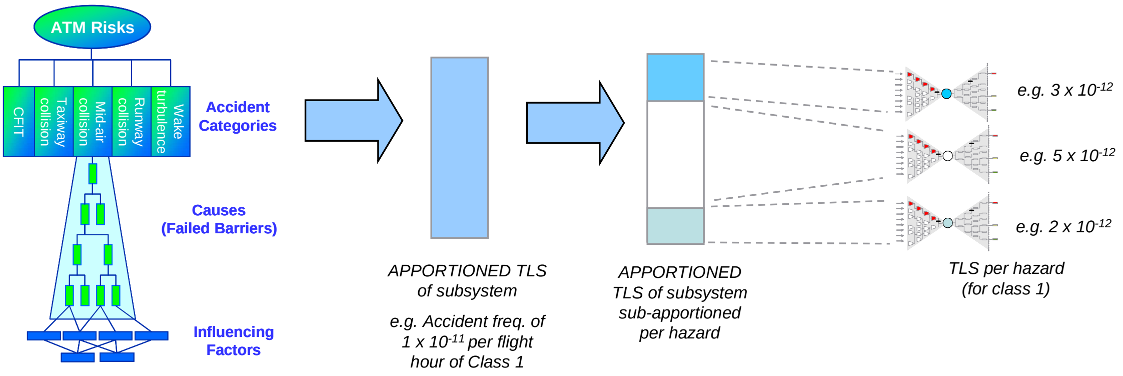


Figure 7: Use of the IRP in the apportionment of a high level TLS

The TLS is implicitly contained within the IRP, and cascaded through the model, allowing a consistently apportioned TLS for the subsystem.

Once the apportioned TLS has been determined, the safety assessment is then carried out as described above in Figure 4. Individual hazards should only make small contributions to the risk of a catastrophic event, as the sum of these contributions are required to meet the apportioned TLS. Within the ESAM methodology the frequency of the catastrophic events is likely to be orders of magnitude lower than the maximum allowable frequency of the hazard (safety objective). This difference is due to barriers in the event tree for example human recovery, environmental factors, providence (luck), or other recovery barriers.

5.2.2.2 Representation of Procedures and Human Factors

A relatively new development within the E-SAM methodology has been the introduction of Procedure Assurance Levels (PALs). These have as yet only been applied to a limited number of cases and are not core to every safety case. These can be used when a procedural failure could lead to a hazard in the system under investigation. The probability of the procedure failure leading to a certain severity of consequence is evaluated, along with the probability and then the required PAL is determined from the table below.

Table 4: PAL Severity Levels

Probability		**Severity**			
		1	2	3	4
	Very possible	PAL1	PAL2	PAL3	PAL4
	Possible	PAL2	PAL3	PAL4	PAL4
	Very unlikely	PAL3	PAL3	PAL4	PAL4
	Extremely unlikely	PAL4	PAL4	PAL4	PAL4

These different PALs have defined requirements in terms of procedure development, testing and implementation in an analogous manner to Software Assurance Levels, as seen below in Table 5.

Software assurance levels as applied to rail systems are described in the document EN 50128 on software for railway control and protection systems [33]. It is not clear there are any direct linkages between the Procedure Assurance Levels as developed in the ESAM and Software Assurance Levels as the history of how PAL has been developed has not been documented within the ESAM.

Both systems determine a level of importance for their respective system (procedure or software) and from this specify a number of quality control elements, which are more stringent for more safety critical systems. These can take the form of additional documentation, testing, validation etc. In the case of EN 50128 this extends to specific recommendations on the software language to be used, types of tests to be performed and standards the developing body should be adhering to. In the case of procedure assurance this can take the form of required documentation, plans or competency of staff.

Within the ESAM, software assurance can also be included and in some studies this has been performed on the same risk matrix for software as procedures, thereby providing a direct link between the systems. In this case some effort has been made to link the PAL with a quantitative safety target, in the form of a risk matrix.

Table 5: Objectives for fulfilling procedure assurance levels

Procedure Assurance Level	Objectives to be fulfilled during the Procedure Life Cycle Phases:				
	i **Definition**	**ii** **Design and Validation**	**iii** **Implementation**	**iv** **Transfer into Operations**	**v** **Operation**
PAL 4 **PAL 3** **PAL 2** **PAL 1**	*i1.* Ensure involvement of relevant operational expertise *i2.* Ensure a minimum set of quality assurance activities *i3.* Establish a proven and well-documented starting point for the definition phase *i4.* Ensure stakeholder acceptance *i5.* Ensure an approved and systematic specification	*ii1.* Establish an acceptable risk level (in quantitative terms) *ii2.* Ensure that HMI has been assessed *ii3.* Ensure suitable validation at different levels *ii4.* Ensure robustness *ii5.* Ensure external expert acceptance *ii6.* Ensure enhanced competence levels of designers *ii7.* Ensure stakeholder acceptance *ii8.* Ensure independency in design and validation	*iii1.* Establish an Implementation Plan which includes quality assurance activities *iii2.* Ensure a minimum set of acceptable quality assurance activities *iii3.* Ensure stakeholder acceptance *iii4.* Ensure training levels *iii5.* Ensure approval at the Corporate level of management *iii6.* Establish evidence of acceptable design maturity *iii7.* Ensure independent auditing of the procedure *iii8.* Ensure corporate level of approval by stakeholders	*iv1.* Ensure that feedback concerning the transfer process is provided to involved staff *iv2.* Ensure documented contingency measures *iv3.* Ensure dissemination of contingency measures *iv4.* Ensure enhanced competence levels of staff to perform the transfer *iv5.* Ensure incremental transfer *iv6.* Ensure approval of the Transfer Plan at management level *iv7.* Ensure stakeholder acceptance of the Transfer Plan *iv8.* Ensure application of an approved and systematic method to verify the transfer process	*v1.* Ensure documentation control *v2.* Establish a reporting system covering occurrences relating to the procedure *v3.* Ensure minimum proficiency levels *v4.* Ensure validity of assumptions *v5.* Ensure promulgation of related incident investigations *v6.* Ensure acceptable performance levels *v7.* Ensure minimum competency levels of staff to operate the procedure *v8.* Ensure that the application of the procedure is reduced to its minimum

Note: each level is additive, so a system requiring PAL1 would require all objectives, whereas PAL4 only requires the objectives in blue to be fulfilled. Reference Guidelines for the Safety Assessment of ATM Procedures (SAAP), SAF.ET1.ST03.1000-SAAP-01-00, edition 0.1, 04/06.

5.2.3 Summary and Comparison with ERA's Study Objectives

1. *The identification of RAC at a technical level and operational/procedural level.*

The ESARR 4 requirements put a high level risk criteria on the ATM system wide behaviour. It is then part of the risk assessment to apportion this target to the sub-system under consideration using tools such as the Integrated Risk Picture. From this apportionment the risk assessment analyses the hazards and calculates safety requirements to ensure the overall sub-system does not exceed its stated risk target.

These requirements are often low level specifications for the performance or reliability of equipment, they could additional be requirements for specific Air Traffic Controller or Pilot training.

To aid this process there is a specific process within the EUROCONTROL SAM methodology for the assessment of procedures, although this has had limited use at present. This takes a qualitative risk approach to a new procedure and then specifies objectives for procedure development, testing and implementation depending on the procedure risk. It is difficult to see how this links with the ESARR 4 requirements.

2. *Are human reliability or semi quantitative techniques such as the SILs or other qualitative rules used to accept human driven actions that allow assessment and acceptance of the systems?*

Human reliability can be explicitly allocated within the EUROCONTROL SAM methodology using Human Reliability Analysis Techniques; in addition a framework exists for the specific analysis of procedures using Procedure Assurance Levels described about in Section 5.2.2.2.

3. *The minimum requirements for performing safety critical tasks should be analysed by studying relevant legislation, guidance or safety management systems. These may also range from quantitative values for the human reliability to description of principles on education or redundancy through check by different people.*

Addressed through the use of human reliability analysis techniques within the risk assessment process and the new system introduced regarding PALs.

We conclude by asking ***could the ESAM/ESSAR4 (or similar) be used in the context of assigning RAC?*** The answer to this question is yes, the ESARR 4 type criteria work as a design target, or whole ATM system criteria. Often the output of an ATM safety assessment would be low level system requirements that the sub-system would then be designed to meet.

5.3 The Chemical Sector and the ARAMIS methodology

5.3.1 What is it and what is it used for?

The chemical sector sets no RAC on a harmonised basis. This is in contrast to the aviation and maritime sectors where harmonised RAC are specified. We surmise that the existence of RAC in the aviation and maritime sectors reflects the fact that these transport modes are international, and that passengers should expect a common level of safety performance regardless of where their journey starts and ends.

Instead, under the Seveso Directive, [10] it is a requirement for a Safety Report and for a Land Use Planning assessment to be completed for top-tier sites.

Given there are no harmonised RAC, the focus of work reported here concerns attempts to develop a common risk assessment framework. This has the objective of ensuring a degree of consistency between Member States risk assessments. One particular piece of work in this area is the **A**ccidental **R**isk **A**ssessment **M**ethodology for **I**ndustrie**S** (ARAMIS).

"The ARAMIS project aims at developing a European harmonised risk-assessment methodology, recommended for use by risk experts and recognized by decision-makers, to evaluate the risk level of industrial establishments by taking into account the accident-prevention tools (safety devices and safety management) implemented by the operators. The development of risk tolerability criteria is not an objective of the project."

ARAMIS is a finished methodology. There is no mandated requirement for the use of ARAMIS within the Seveso Directive and therefore its use is optional.

5.3.2 What it includes

ARAMIS addresses the following aspects of safety risk assessment:

1. Identification of hazards
2. Identification of safety barriers and assessment of their performance
3. Evaluation of safety management efficiency to safety barrier reliability
4. Identification of reference accident scenarios
5. Assessment and mapping of the risk severity of reference scenarios
6. Evaluation and mapping of the vulnerability of the plant's surroundings

We address each in turn below, and concentrate on those areas that are novel and address areas have relevance to the railway sector.

With regard to steps 5 and 6, ARAMIS requires the analysis of the effects of a product release to be considered. This process requires thermal radiation, blast and toxic effects to be geographically mapped onto surrounding areas and then for the consequences to be established in terms of loss of life and other unwanted outcomes. There is no direct parallel in terms of railway risks (unless transport of dangerous goods is to be considered).

5.3.2.1 Identification of Hazards

The ARAMIS seven step process for hazard identification is summarised below.

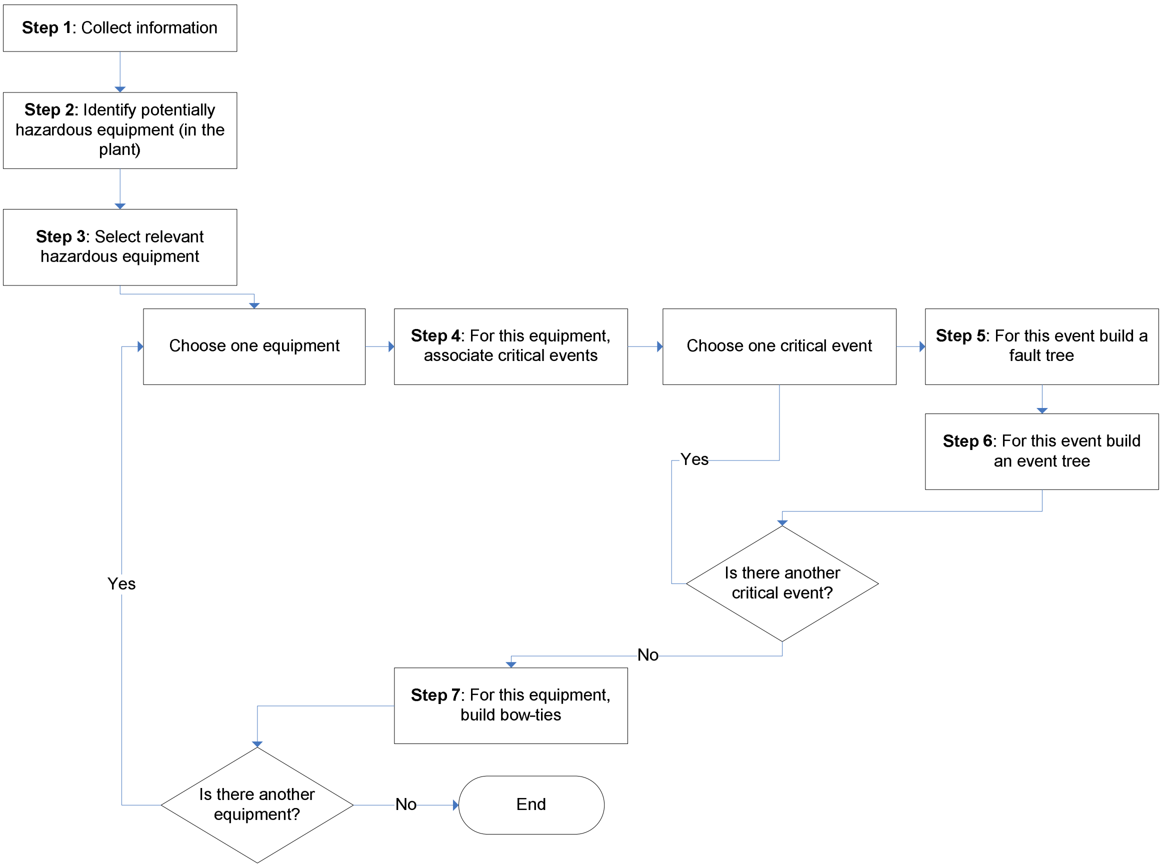

Step 1: Collect information
Step 2: Identify potentially hazardous equipment (in the plant)
Step 3: Select relevant hazardous equipment
Choose one equipment
Step 4: For this equipment, associate critical events
Choose one critical event
Step 5: For this event build a fault tree
Step 6: For this event build an event tree
Yes
Is there another critical event?
Yes
No
Step 7: For this equipment, build bow-ties
Is there another equipment?
No
End

Figure 8: ARAMIS Hazard Identification Process

Steps 1 through 3 have the objective of ensuring the relevant equipments are selected for study. The methodology requires the plant to be categorised based on the type of hazardous substances within it, together with a list of equipment items containing those substances. Equipment within the plant is selected for further analysis if the mass of a hazardous substance is equal to or higher than a threshold value, or there is significant escalation potential. Specific instructions are provided to ensure that critical equipment is selected on a consistent basis regardless of who is conducting the analysis.

Step 4 provides a methodology for associating critical events (hazards) to the critical equipment selected for further study. It achieves this via a matrix. One axis of the matrix is a critical event (such as explosion, fire etc) and the other is an equipment type. The matrix is pre-populated such that the analyst can read directly the type of critical event that is associated with that equipment.

Step 5 requires the development of a fault tree. A generic set of fault trees has been produced (one fault tree for each critical event) to support the ARAMIS methodology. The fault trees are intended to act as a checklist of possible causes which the analyst can edit to remove unnecessary causes, or alternatively to add additional causes as appropriate.

Step 6 requires the development of an event tree. The process is simplified by a methodology and set of tools that partly automates the process. The starting point of the construction process is the fault tree from Step 5, in particular the critical event. The construction process requires the analyst to answer questions that defines the next stage in the escalation process. The process is complete when the "*dangerous phenomena*" (e.g. a poolfire) are established.

Step 7 is the integration of the preceding steps to create a bow-tie model. Note that the methodology requires that the construction of the bow-tie diagrams assume no safety systems (including safety management systems) are installed or that they are ineffective.

5.3.2.2 Assigning Performance Levels to Safety Functions and Barriers

ARAMIS [11] defines a safety function as a "*technical or organisational function*" and the safety barrier as the "*physical or engineered system or human action*" which implement the safety function.

The next stage in the ARAMIS process is to identify safety functions and barriers which is achieved by inspection of the bow-tie. (Guidance is provided to aid this task.)

Once identified the safety function/barrier requires its effectiveness to be established (the degree of effectiveness is called a *level of confidence*). The allocation of a level of confidence is closely related to concept of SIL. In this process technical/engineered barriers are defined as being either type A or type B.

A sub-system is type A if:

- The failure modes of all components are well defined, AND the behaviour of the subsystem under fault conditions can be completely determined, AND dependable failure data from field experience exists for the subsystem, sufficient to show that the required target failure measure is met.

A sub-system is type B if:

- The failure mode of at least one component is not well defined, OR the behaviour of the subsystem under fault conditions cannot be completely determined, OR no dependable failure data from field experience exists for the subsystem, sufficient to show that the required target failure measure is met.

The following levels of confidence can be allocated:

Table 6: Level of Confidence Allocation

Type A

Safe Failure Fraction	Fault Tolerance		
	0	1	2
< 60%	LC1	LC2	LC3
60% - < 90%	LC2	LC3	LC4
90% - < 99%	LC3	LC4	LC4
>= 99%	LC4	LC4	LC4

Type B

Safe Failure Fraction	Fault Tolerance		
	0	1	2
< 60%	N/A	LC1	LC2
60% - < 90%	LC1	LC2	LC3
90% - < 99%	LC2	LC3	LC4
>= 99%	LC3	LC4	LC4

Safe failure fraction describes the ratio of fail safe frequency to total failure frequency.

The ARAMIS methodology allows the following performance criteria to be allocated:

Table 7: Level of Confidence Values

Low Demand Based Operation

Level of Confidence	Average probability of failure to perform function (IEC 61508)
LC4	>=10^{-5} to < 10^{-4}
LC3	>=10^{-4} to < 10^{-3}
LC2	>=10^{-3} to < 10^{-2}
LC1	>=10^{-2} to < 10^{-1}

High Demand/Continuous Operation

Level of Confidence	Probability of dangerous failure per hour (IEC 61508)
LC4	>=10^{-9} to < 10^{-8}
LC3	>=10^{-8} to < 10^{-7}
LC2	>=10^{-7} to < 10^{-6}
LC1	>=10^{-6} to < 10^{-5}

Pre-defined performance levels are allocated for some safety barriers and functions. In these cases, the performance value can be extracted directly from the pre-defined list, short cutting the process above.

A similar process is applied for human errors and ARAMIS has proposed the following baseline values:

- Where the human barrier is of a preventative nature or part of a normal operation, a probability of failure on demand of 10^{-2} (LC2) is suggested
- Where the human barrier requires a specific intervention, a probability of failure on demand of 10^{-1} (LC1) is suggested

Within ARAMIS these performance allocations are referred to as a ***design barrier level of confidence***; that is the level of confidence that the safety barrier or function can achieve "on the drawing board".

5.3.2.3 Evaluation of Safety Management Efficiency

The next stage of the process suggests that in practice the design barrier level of confidence may not be reached. The concept forwarded is thus:

- A safety barrier or function has a design barrier level of confidence that may be achieved under optimal conditions
- In practice the design barrier level of confidence may not be reached due to deficiencies associated an organisations safety management system and culture (for example sub-optimal maintenance procedures, etc). The realised performance considering these aspects is termed the ***operational barrier level of confidence***.

ARAMIS proposes that such aspects can be measured and assessed through audit and an audit process has been developed for this purpose, as indicated by the diagram below.

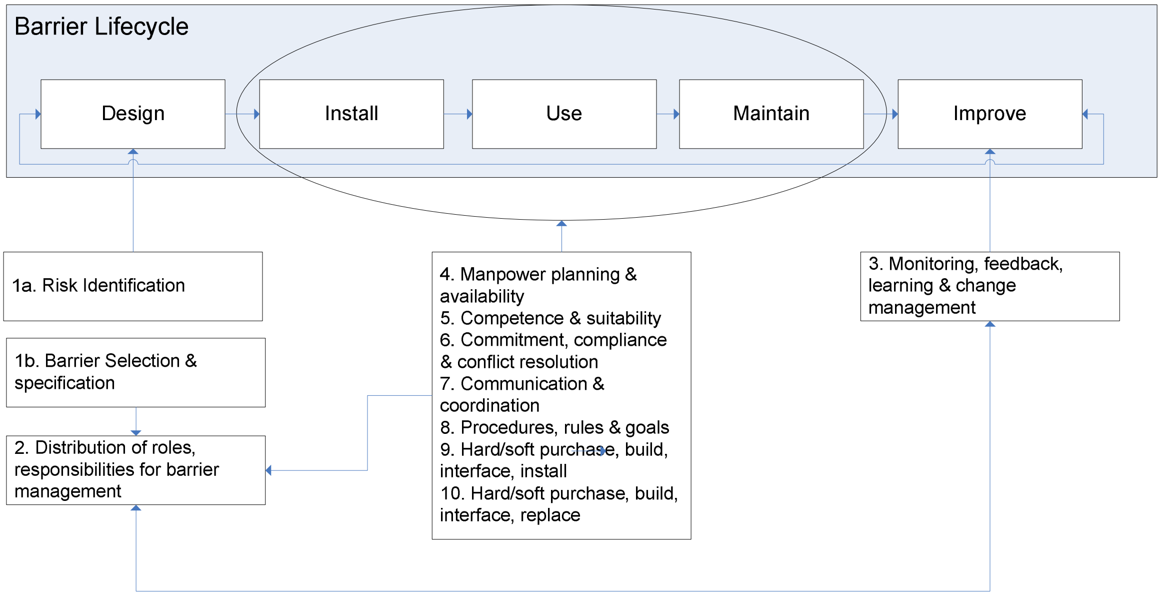

Barrier Lifecycle
Design
Install
Use
Maintain
Improve
1a. Risk Identification
1b. Barrier Selection & specification
2. Distribution of roles, responsibilities for barrier management
4. Manpower planning & availability
5. Competence & suitability
6. Commitment, compliance & conflict resolution
7. Communication & coordination
8. Procedures, rules & goals
9. Hard/soft purchase, build, interface, install
10. Hard/soft purchase, build, interface, replace
3. Monitoring, feedback, learning & change management

Figure 9: ARAMIS Safety Management Assessment

The audit process addresses each of the elements 1 through 10, and for each an audit protocol is developed and described in terms of critical success factors and provided with sample questions. Template tools are available to assist with the audit. The literature to support the audit is comprehensive and described in [12].

We note however that the audit is scored and leads to management system and safety culture ratings. These ratings are applied to the design barrier level of confidence derived in Section 5.3.2.1 leading to an operational barrier level of confidence.

5.3.2.4 Identification of Reference Accident Scenarios

This part of the ARAMIS methodology provides a means of prioritising the bow-ties to identify those that should be subject to a formal severity analysis. Two methods are proposed: a method that requires a formal quantification of the fault tree; a method that estimates directly the frequency of a critical event.

The formal quantification should be completed through the identification of specific failure data or, as an alternative the methodology [13] provides a summary of generic data that may be used (which includes a thorough review of human error data). Should this not be appropriate the methodology also identifies the frequency of critical events (hazards) directly from accident and incident data.

The output of the quantified bow-tie is used in conjunction with the risk matrix provided below. This process is applied by directly plotting a critical event’s frequency and consequence (as established from the bow-tie analysis) onto the risk matrix below. Scenarios that fall into either the red or yellow zones are considered “high risk” and taken forward for severity modelling (steps 5 and 6 of the ARAMIS methodology, as discussed in 5.3.2).

10^{-2} / year	🟩	🟥	🟥	🟥
10^{-3} / year	🟩	🟨	🟥	🟥
10^{-4} / year	🟩	🟨	🟨	🟥
10^{-5} / year	🟩	🟩	🟨	🟨
10^{-6} / year	🟩	🟩	🟩	🟨
10^{-7}/ year	🟩	🟩	🟩	🟩
10^{-8} / year	🟩	🟩	🟩	🟩
	C1	C2	C3	C4

Figure 10: ARAMIS Risk Matrix

Consequence classes are defined as follows:

Table 8: Risk Consequence Classes

CONSEQUENCES			CLASS
Domino Effect	Effect on human target	Effect on environment	Ranking
To take into account domino effects, the class of consequence attributed to the studied dangerous phenomenon will be increased to the class of the secondary phenomenon that the first can bring about by domino effect	No injury or slight injury with no stoppage of work	No action necessary	C1
	Injury leading to an hospitalisation > 24 hours	Serious effects on environment, requiring local intervention	C2
	Irreversible injuries or death inside the site. Reversible injuries outside the site	Effects on environment outside the site, requiring national action	C3
	Irreversible injuries or death outside the site	Irreversible effects on the environment outside the site	C4

5.3.3 Other Relevant Areas

5.3.3.1 Apportioning Performance Requirements to Safety Functions and Barriers

The ARAMIS methodology introduces a process for establishing the required level of confidence a safety function/barrier must achieve in order that an overall risk target is met (derived from IEC 61508, see Section 6.3). Its use is particularly relevant to the design stage of a project when specifying safety requirements and performance targets. Alternatively, it can also be used for existing equipment, in order to verify if the safety systems are sufficient.

An extract is presented in Figure 11 below. The parameters to the left of the diagram define:

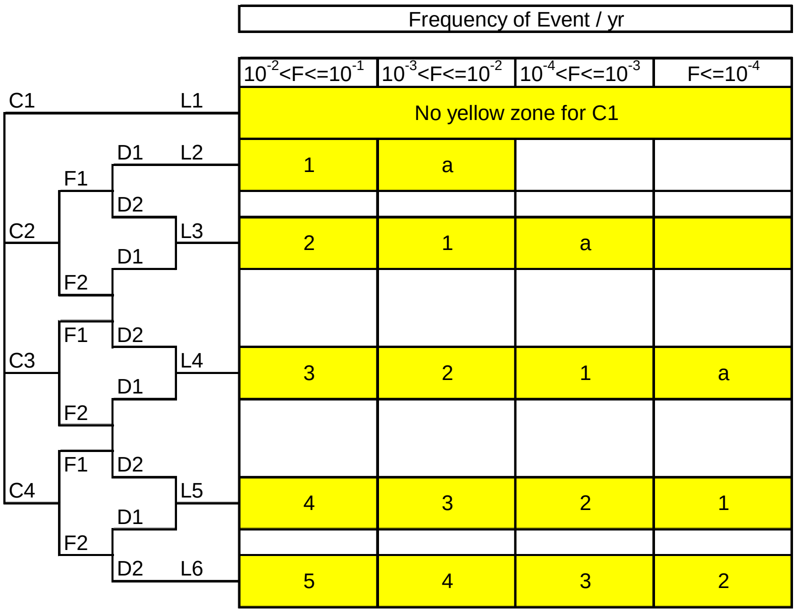
- Consequence (see Table 8)
- Hazard exposure (F1 meaning less than 10% exposure and F2 meaning more than 10% exposure)
- The possibility that the consequences are avoided by intervention or evacuation (D1 meaning that an intervention and/or evacuation plan is in place and can be executed, or D2 in cases where this is not likely).

These parameters are assigned leading to an outcome scenario L1 to L6.

The frequency of the event leading to this outcome is read across the top of the diagram and the intersection then defines the level of confidence required for the safety function/barrier.

For example, an outcome L4 may be determined by application of this process. The error leading to this outcome may be a human error with an error rate of 10^{-1} per year. It can be seen from the diagram that the intersection of event frequency 10^{-1} per year and outcome scenario L4 requires a safety function/barrier with a level of confidence 3 to ensure that the risk lies within the yellow (tolerable) sector of the risk matrix.

The diagram is fixed relative to a specific risk matrix.



	Frequency of Event / yr			
	10^{-2}<F<=10^{-1}	10^{-3}<F<=10^{-2}	10^{-4}<F<=10^{-3}	F<=10^{-4}
L1	No yellow zone for C1			
L2	1	a		
L3	2	1	a	
L4	3	2	1	a
L5	4	3	2	1
L6	5	4	3	2

Figure 11: ARAMIS Level of Confidence Allocation

5.3.3.2 Performance Evaluation of Safety Functions and Barriers

Once a performance requirement is established, ARAMIS provides a technique to determine whether the required level of confidence is achieved by the safety barriers put in place. Considering the example above, the following may be identified and proposed as mitigation.

Table 9: Safety Functions and Barriers

Safety Function	Safety Barrier
To prevent operator error	Training of the operator. Indications on pipes to identify them. Procedure (check whether pipe is empty with pressure detection devices)
To limit the product release	Measure pressure in the pipe. Logic controller. One automatic shut –down valve at each extremity of the pipe

In our assessment we may assume the hazardous scenario will be avoided if the operator error is eliminated. The barrier to mitigate this may be training. [14] suggests that a level of confidence 1 may be assigned to “operator responds to an alarm with procedures, low stress, known event and 15 min to answer” which may be appropriate in these circumstances. Therefore the barrier to achieve this safety function has a level of confidence 1.

The safety barriers to limit the product release require an assessment of the architecture of the system. This may be as follows:

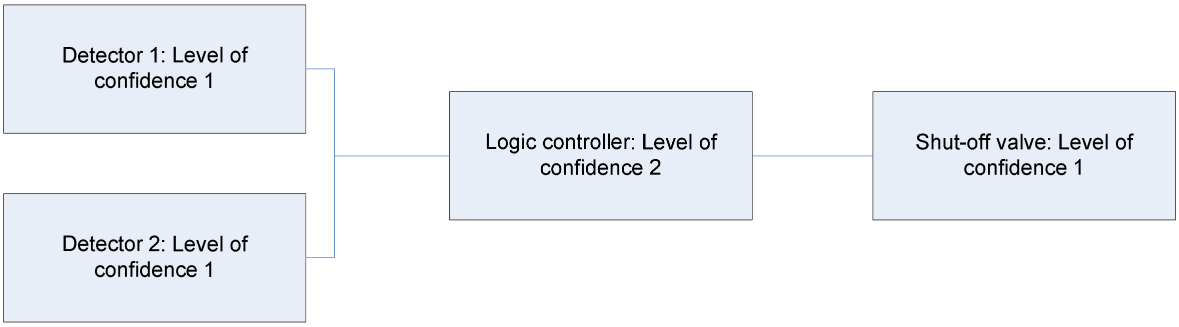

Detector 1: Level of confidence 1
Detector 2: Level of confidence 1
Logic controller: Level of confidence 2
Shut-off valve: Level of confidence 1

Figure 12: ARAMIS Level of Confidence Assessment

The methodology suggests that a level of confidence can be no higher than the weakest link in the chain. In this case, the detection sub-system is one fault safe (because there are two detectors in parallel; ref Table 6) and therefore a level of confidence 2 can be allocated to this sub-system. The weakest link in the chain is thus the shut-off value, and an overall level of confidence 1 would be selected for this safety function.

According to this methodology if the safety functions are independent of each other (which in this case they are) they can be combined by adding the levels of confidence of each safety function. Hence a level of confidence 2 (prevent operator error = 1 and limit product release = 1). This fails to meet the requirement.

To improve the safety performance for this sub-system, the safety function to limit the release could be improved by making the shut-off valve one fault safe leading, or by procuring alternative equipment with a better safe failure fraction. If this were achieved a level of confidence 2 may be applicable leading to an overall combined level of confidence 3.

(Note that this is a simplified example, and further details are provided in [15]. We also point out that we are reporting on the methodology and have not validated the mathematics that supports it.)

5.3.4 What is excluded

The Chemical sector does not specify RAC on a harmonised level.

5.3.5 Summary and Comparison with ERA's Study Objectives

1. *The identification of RAC at a technical level and operational/procedural level.*

RAC are not specified within the Seveso Directive; there are no harmonised RAC within this industry sector. ARAMIS exists as a common risk assessment methodology within this sector, although its use is optional.

2. *Are human reliability or semi quantitative techniques such as the use of SILs or other qualitative rules used to accept human driven actions that allow assessment and acceptance of the systems?*

In the context of "assessment", ARAMIS has dealt with all the topics listed here. Human error data points are suggested and a comprehensive system for assigning levels of confidence is documented.

There are no specific guidelines regarding acceptance.

3. *The minimum requirements for performing safety critical tasks should be analysed by studying relevant legislation, guidance or safety management systems. These may also range from quantitative values for the human reliability to description of principles on education or redundancy through check by different people.*

ARAMIS contains quantitative values for human reliability.

In addition, a process for assessing safety management and culture is proposed. Within this system, and under the topic area "Competence and Suitability", guidance is provided on what controls may be put in place for persons completing critical tasks. These however are concerned with issues of a general nature such as job safety analysis and task analysis and are therefore similar in content to a number of audit techniques; in other words they reinforce existing practices in this area, rather than introduce novel approaches.

We conclude by asking ***could ARAMIS (or similar) be used in the context of assigning RAC?*** ARAMIS (as far as we are aware) has not been used as a mechanism for setting RAC, however the theory underpinning it is common to other techniques (described in this report) that have been used for this purpose. ARAMIS contains a number of tools and techniques that may address some of ERA's requirement, for example the Level of Confidence approach to the definition and assessment of safety barrier performance.

5.4 The Railway Safety Risk Model (Great Britain)

5.4.1 What is it and what is it used for?

The SRM is a railway risk modelling tool. It is maintained by the Rail Safety and Standards Board (RSSB) and made available, via the use of simplified templates, to organisations having a need to use it. It is used in GB only. Its purpose includes:

1. To provide a focus for key risk areas that require further investigation
2. To help the development of the industry's Strategic Safety Plan, [16]
3. To provide input into safety decision making and cost-benefit analysis
4. The preparation of risk assessments for train operating companies and other risk assessments (via the use of simplified templates)
5. The assessment of change proposals

As indicated in bullet 2, the SRM can be used to set RAC and to judge the longer term safety trends of GB's railways. For example:

- Passenger safety metric of 1.070 Fatalities and Weighted Injuries (FWI) per billion passenger kilometres
- Workforce safety metric of 0.134 FWI per million worker hours

These were set with reference to the SRM in response to the Government's High Level Output Specification requirements. In addition, by modelling the planned introduction of new technology over time the SRM can predict safety trajectories.

It can also be used to dissect the safety performance of GB's railways in a number of ways. This includes on a hazard by hazard basis, and/or at the level of hazard precursors such as Signals Passed At Danger (SPADS, which is also a defined CSI). It thus provides a link between CSIs and CSTs.

An example output is provided below. Further uses of the SRM and outputs are provided at [16].

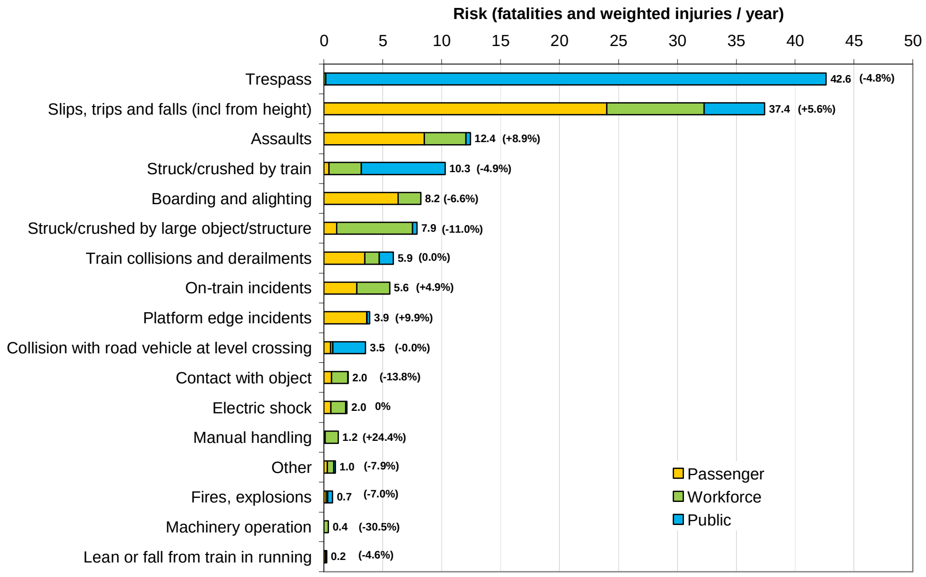


Figure 13: SRM Output

The SRM does not include any features that model the impacts (negative or positive) of differences in safety management and/or culture between organisations (compare with ARAMIS which has addressed this). This omission is not critical at a national level where the same rules apply to all. However, in an international context, when safety rules, safety performance and safety culture may differ, this may be significant.

5.4.2 What it includes

The SRM comprises a set of fault tree, event tree and consequence models representing 120 hazardous events on the railway. These are split into Train Accidents (e.g derailments), Train Movement Accidents (e.g. collision with person on track) and Non Movement Accidents (e.g. slips, trips). An extract of the derailment model is provided below.

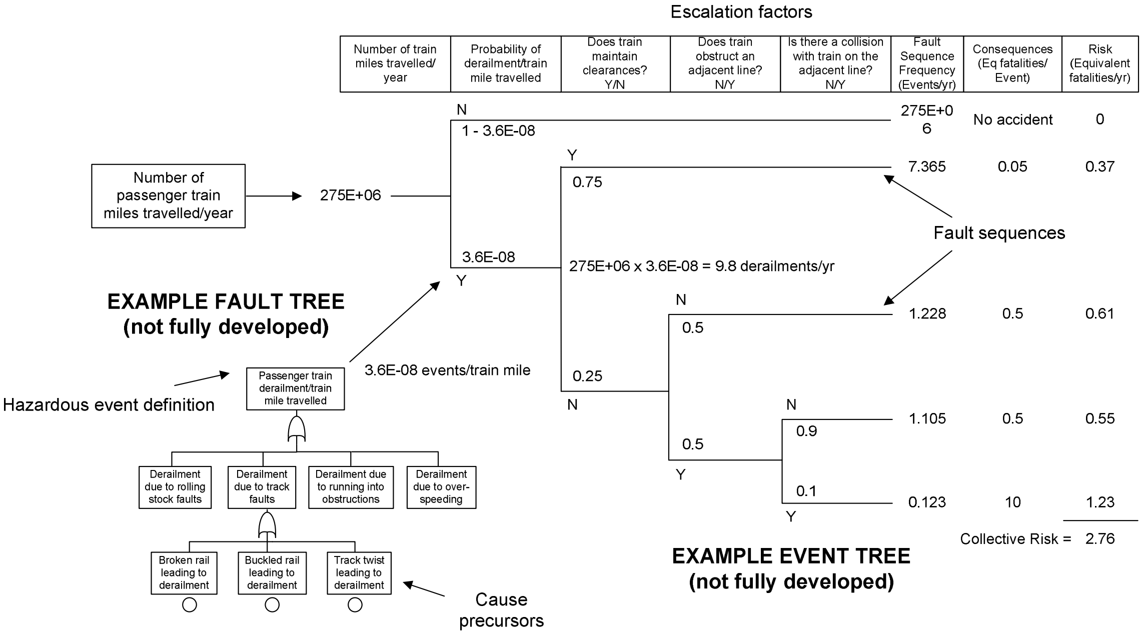

Escalation factors
Number of train miles travelled/ year
Probability of derailment/train mile travelled
Does train maintain clearances? Y/N
Does train obstruct an adjacent line? N/Y
Is there a collision with train on the adjacent line? N/Y
Fault Sequence Frequency (Events/yr)
Consequences (Eq fatalities/ Event)
Risk (Equivalent fatalities/yr)
Number of passenger train miles travelled/year
275E+06
N
1 - 3.6E-08
3.6E-08
Y
Y
0.75
275E+06 x 3.6E-08 = 9.8 derailments/yr
0.25
N
N
0.5
0.5
Y
N
0.9
0.1
Y
275E+06
No accident
0
7.365
0.05
0.37
Fault sequences
1.228
0.5
0.61
1.105
0.5
0.55
0.123
10
1.23
Collective Risk = 2.76
EXAMPLE EVENT TREE (not fully developed)
EXAMPLE FAULT TREE (not fully developed)
3.6E-08 events/train mile
Hazardous event definition
Passenger train derailment/train mile travelled
Derailment due to rolling stock faults
Derailment due to track faults
Derailment due to running into obstructions
Derailment due to over-speeding
Broken rail leading to derailment
Buckled rail leading to derailment
Track twist leading to derailment
Cause precursors

Figure 14: Derailment Analysis

The models are developed to be generic (that is there is one model for each hazard and scaled based on national average data).

The modelling contains technical (equipment) and operational (human) failures. Where possible, data to populate these events are extracted from the Safety Management Information System (SMIS). This is an industry database populated by all Railway Group members. Where SMIS does not contain data for an item that is to be modelled, one of a number of alternative techniques may be applied. These include expert judgement and additional predictive modelling as required.

Specifically for human errors, the HEART technique is preferred because it is easy to use and has been found to provide reasonable predictions when applied correctly.

The consequences in terms of loss of life and injury are similarly established from real data, where possible. However specific modelling may be required in order to establish consequences for rare events, where there is little prior history.

It can be seen from the modelling structure that CSIs are specifically included, such as broken rails in this example, therefore providing a link between these CSIs and overall system risk.

5.4.3 What is excluded

The SRM is structured to assess the overall average incidence of railway hazards on the National mainline rail network. It is not organised to allow specific routes to be studied. However, to enable Train Operating Companies (who operate specific routes) to use the SRM, the RSSB has developed templates that can be used. The templates require the user to identify the specific details of their operation (such as number of miles travelled) and other critical factors. Using these data a risk profile is generated for that particular operation.

The SRM and other related industry guidance does not contain a qualitative method that can be applied to demonstrate (for example) that:

> *For technical systems where a functional failure has a credible direct potential for a catastrophic consequence, the associated risk does not have to be reduced further if the rate of that failure is less than or equal to 10^{-9} per operating hour*

However in this regard Safety Integrity Levels may be used as an input during an expert judgement session, in the absence of other data. Alternatively, we have reported on an equivalent technique that is contained within ARAMIS.

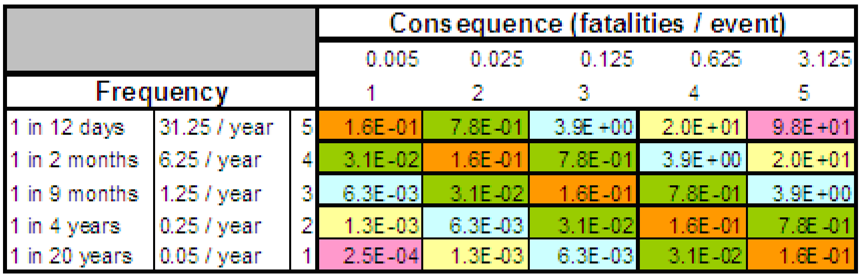
5.4.4 Other Relevant Areas

5.4.4.1 The Risk Matrix

A risk matrix is a commonly used tool, and one which could be adopted to support harmonised RAC or decision making. Useful guidance is provided relating to the means of scaling a risk matrix either in a qualitative or semi-quantitative sense.

To demonstrate, we consider the following risk matrix in which frequency and consequence are ***separated by a common factor*** (in this case a factor of 5). In this case we can estimate the value of collective risk indicated by the matrix as the product of frequency / year and consequence / event. This is shown below:

Table 10: Quantified Risk Matrix



			Consequence (fatalities / event)				
			0.005	0.025	0.125	0.625	3.125
Frequency			1	2	3	4	5
1 in 12 days	31.25 / year	5	1.6E-01	7.8E-01	3.9E+00	2.0E+01	9.8E+01
1 in 2 months	6.25 / year	4	3.1E-02	1.6E-01	7.8E-01	3.9E+00	2.0E+01
1 in 9 months	1.25 / year	3	6.3E-03	3.1E-02	1.6E-01	7.8E-01	3.9E+00
1 in 4 years	0.25 / year	2	1.3E-03	6.3E-03	3.1E-02	1.6E-01	7.8E-01
1 in 20 years	0.05 / year	1	2.5E-04	1.3E-03	6.3E-03	3.1E-02	1.6E-01

It is important to note that the diagonals are of (approximately) equal magnitude. If we wish to use the risk matrix in a qualitative sense (maybe to prioritise the importance of individual hazards), then it is critical that the weighing allocated maintains this relationship. To achieve this a qualitative risk matrix is complied by ***adding*** the frequency and consequence rankings.

Table 11: Semi-Quantified Risk Matrix

			Consequence (fatalities / event)				
			0.005	0.025	0.125	0.625	3.125
Frequency			1	2	3	4	5
1 in 12 days	31.25 / year	5	6	7	8	9	10
1 in 2 months	6.25 / year	4	5	6	7	8	9
1 in 9 months	1.25 / year	3	4	5	6	7	8
1 in 4 years	0.25 / year	2	3	4	5	6	7
1 in 20 years	0.05 / year	1	2	3	4	5	6

In this case the diagonals are equal reflecting an equal level of risk. This can be contrasted with the practice of multiplying the frequency and consequence rankings which would result in a leading diagonal with values 5, 8, 9, 8 and 5.

To define the appropriate risk boundaries we need to recognise that risk matrices record collective risk, and that normally risk criteria are based on levels of individual risk. For example, if the RAC to an individual train passenger are defined as:

1. Intolerable if the probability of fatality per year exceeds 1E-04 (1 in 10,000 per year);
2. Tolerable if the probability of fatality per year lies in the region 1E-04 to 1E-06 (1 in 10,000 to 1 in 1,000,000 per year);
3. Broadly acceptable if the probability of fatality per year is less than 1E-06 (1 in 1,000,000 per year).

If we assume a passenger makes 2 journeys per day for 250 days per year, and that in total 10,000,000 passenger journeys are made on an annual basis, then that passenger is exposed to (500/10,000,000 = 5.0E-05) of the total passenger risk. We can apply this factor to each collective risk matrix point to calculate the individual risk/passenger/year (e.g. for risk rank 6; 1.6E-01 * 5.0E-5 = 8.0E-06, etc). Applying this for all risk points on the matrix, and comparing with the RAC, results in the risk matrix below:

Table 12: Risk Matrix with Acceptance Boundaries

			Consequence (fatalities / event)				
			0.005	0.025	0.125	0.625	3.125
Frequency			1	2	3	4	5
1 in 12 days	31.25 / year	5	8.0E-06	3.9E-05	2.0E-04	1.0E-03	4.9E-03
1 in 2 months	6.25 / year	4	1.6E-06	8.0E-06	3.9E-05	2.0E-04	1.0E-03
1 in 9 months	1.25 / year	3	3.2E-07	1.6E-06	8.0E-06	3.9E-05	2.0E-04
1 in 4 years	0.25 / year	2	6.5E-08	3.2E-07	1.6E-06	8.0E-06	3.9E-05
1 in 20 years	0.05 / year	1	1.3E-08	6.5E-08	3.2E-07	1.6E-06	8.0E-06

Finally, if this approach to establishing risk boundaries is used, it should be remembered that we have established the boundaries applicable when all hazards and risks are summated (i.e. the total summated individual risk). Whilst it is therefore possible to say that if a hazard has a risk that lies in the red region it is intolerable, it is not necessarily correct to say that because all hazards are in the tolerable region, that the total summated individual risk is also tolerable.

For example, we may have 12 hazards which fall into risk rank 7 (3.9E-05). Although individually each is in the tolerable region when combined the total risk is approximately (12 * 3.9E-5 = 4.7E-4) which is in the intolerable region. (ERA may want to note this limitation in respect of the technical system criteria of 10^{-9} per operating hour that is specified.)

5.4.4.2 Safety Critical Work

The principals relating to Safety Critical Work (SCW) [17] are task and competence based. Safety critical tasks are specifically identified in relation to activities associated with: vehicles used in a transport system; in relation to a transport system (e.g. maintenance); in relation to training.

A competence and fitness system is in place which requires that a SCW task controller is appointed with responsibilities that include:

1. Ensuring that the person undertaking the safety critical task is assessed as competent and fit to carry out that work
2. Ensuring that an accurate and up to date training record is maintained and available for inspection
3. Ensuring that a competence monitoring system is in place
4. Bing equipped to identify and review an individual’s competence should they have reason to, or should there be significant change in relation to the matters to which the competence assessment relates
5. Acting in the best interests in relation to the health and safety of persons on the transport system
6. Acting in concert and in co-operation with other SCW task controllers

An additional requirement relates to the assessment of fatigue, and to ensure that a system is in place to prevent SCW being completed by persons so fatigued that his/her health or safety or the health and safety of other persons on a transport system could be affected. We note the existence of tools and techniques to complete a fatigue assessment, but have not considered them further within this study.

These fatigue systems are usually rules based and include requirements that include maximum driving time (for train drivers), frequency of rest breaks etc. The use of fatigue monitoring and the fatigue risk index calculation tool [18] is common practice.

5.4.5 Summary and Comparison with ERA’s Study Objectives

1. *The identification of RAC at a technical level and operational/procedural level.*

The GB rail sector applies RAC that are consistent with the Railway Safety Directive and associated Commission Decisions, including NRVs and CSTs. In addition, the SRM is used to set additional RAC metrics in relation to the HLOS for example. There are no lower level targets specified on either a technical or operational level. However, information on the absolute or relative contribution of all 120 modelled railway hazards and their precursors can and are derived for risk monitoring and mitigation purposes.

2. *Are human reliability or semi quantitative techniques such as the SILs or other qualitative rules used to accept human driven actions that allow assessment and acceptance of the systems?*

SILs and other consensual standards may be used during an expert judgement session to supplement areas where existing data does not exist for technical systems.

Specifically in relation to human errors, HEART modelling is the preferred method of error prediction in cases where operational data is not available. It may be possible to infer therefore that scaling factors contained with the HEART technique (such as “little or no independent checking of testing of output” having a x 3 Error Producing Factor).

3. *The minimum requirements for performing safety critical tasks should be analysed by studying relevant legislation, guidance or safety management systems. These may also range from quantitative values for the human reliability to description of principles on education or redundancy through check by different people.*

Safety critical tasks are controlled through a competency / education based system as described in Section 5.4.4.2. It is our experience, through the conduct of audits, that the implementation of these systems is tightly controlled within individual safety management systems and closely follows the legislation, [17]. Additional risk assessment and management techniques may be used by individual companies to seek to further control the risks associated with SCW. This may involve task analysis or other methods, but this is at the discretion of an individual organisation.

There are additional rules governing fatigue management, rostering and working hours which include specific tools and techniques that address this topic [18].

We conclude by asking ***could the SRM (or similar) be used in the context of assigning RAC?*** The answer to this question is clearly yes, because it is used for this purpose within GB. However, as discussed earlier, the SRM is GB specific and would not be directly applicable in other Member States.

The context of its use within GB is one which requires global or high level RAC to be achieved rather than specifying low level RAC. It is possible however that the SRM could derive RAC at the major hazard level, or perhaps at a precursor level and, in some cases at the CSI level.

This could be used with a complementary tool, such as a risk matrix, to estimate whether the hazard level RAC could be achieved by a system, or number of systems, with a specific low level RAC.

Finally it is the case than an individual Member State's risk model is applicable to that particular environment and safety culture. It is feasible that this could be addressed by setting the benchmark performance level relative to the environment and culture in that Member State (through assessment) using a suitable scored assessment tool and making a similar assessment for remaining Member States. This is similar to the process applied within ARAMIS.

5.5 Maritime Formal Safety Assessment

5.5.1 What is it and what is it used for?

Formal Safety Assessment (FSA) [19] is a structured and systematic methodology, aimed at enhancing maritime safety, including protection of life, health, the marine environment and property through the use of risk analysis and cost benefit assessment. It has been developed by the International Maritime Organisation (IMO), a specialised agency of the United Nations.

FSA is applied to generic ship designs, not individual ships. Risk reduction measures, if deemed by the FSA as needed are implemented as prescriptive rules for that ship type. This means there is no need for any low level RAC. The FSA was chosen as an alternative to performing a safety case for each individual ship; a safety case approach was thought to be impractical for merchant ships due to the international nature of shipping operations and the use of flag of convenience.

The prescriptive rules determined by the FSA form only part of the overall system that governs ship safety. In addition individual ships are classified by a maritime classification society; the classification societies are organisations that establish and apply technical standards in relation to the design, construction and survey of marine related facilities including ships and offshore structures [34]. The “class rules” are themselves risk based. The classification process consists of:

- A technical review of the design plans and related documents for a new vessel to verify compliance with the applicable rules;
- Attendance at the construction of the vessel in the shipyard by a classification society surveyor(s), and at the relevant production facilities that provide key components such as the steel, engine, generators and castings, to verify that the vessel is constructed in accordance with the classification rules;
- Upon satisfactory completion of the above, the shipowner’s request for the issuance of a class certificate. This is considered by the relevant classification society and, if deemed satisfactory, the assignment of class will be approved and a certificate of classification issued;
- Once in service, the owner must submit the vessel to a clearly specified program of periodical class surveys, carried out onboard the vessel, to verify that the ship continues to meet the relevant rule conditions for continuation of class.

Classification is one element within a network of maritime safety partners. Other elements are parties such as the shipowner, the shipbuilder, the flag State, port States, underwriters, shipping financiers, and charterers among others.

Risk criteria are not formally defined within the FSA methodology however individual risk criteria have subsequently been agreed based on the UK HSE criteria. These were chosen as they were believed to be technically the best available at the time. These are defined per ship-year:

- Maximum tolerable fatality risk for crew members 10^{-3} annually
- Maximum tolerable fatality risk for passengers or public 10^{-4} annually
- Negligible fatality risk 10^{-6} annually

These targets are not particularly strict. Instead when considering a comprehensive FSA on new ships a stronger target should be used:

- Maximum tolerable fatality risk for crew members 10^{-4} annually

- Maximum tolerable fatality risk for passengers or public 10^{-5} annually

Societal risk should also be considered, and this is done through the use of F-N curves.

If residual risks are lower than the tolerable estimates, but above negligible a CBA process should be used to evaluate which if any risk reducing measurers should be implemented. From recent FSAs carried out the cost of averting a fatality is in the region US$1.5m to US$5m.

5.5.2 How was it derived?

The individual risk criteria maximum tolerability limits stated have been derived from the UK HSE figures. These were chosen as they were believed to be technically the best available at the time.

- Maximum tolerable fatality risk for crew members 10^{-3} annually
- Maximum tolerable fatality risk for passengers or public 10^{-4} annually
- Negligible fatality risk 10^{-6} annually

With target risks set one order of magnitude more stringent.

These risks are based [20] on historical frequencies of individual risk in the high risk industries. Namely:

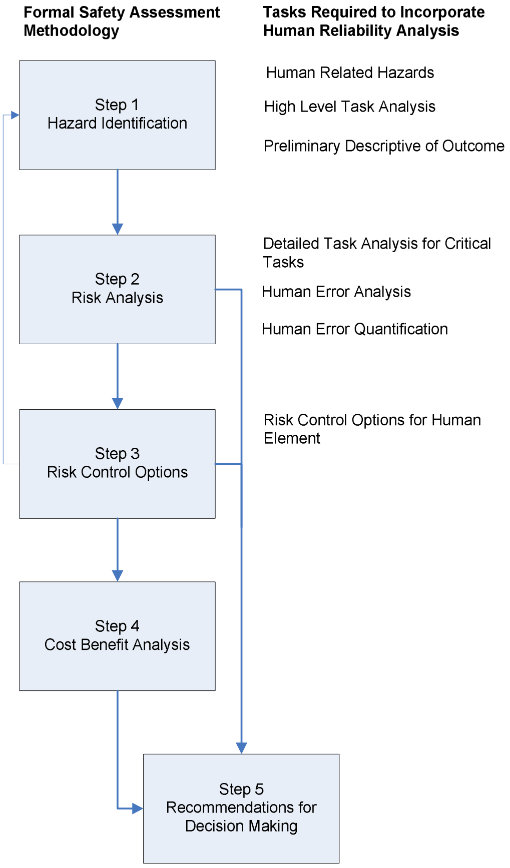
Table 13: Annual risk of death from industrial accidents to employees for various industry sectors (Health and Safety Commission, 2001), reproduced from [20].

Industry sector	Annual risk	Annual risk per million
Fatalities to employees	1 in 125000	8
Fatalities to the self-employed	1 in 50000	20
Mining and quarrying of energy producing materials	1 in 9200	109
Construction	1 in 17000	59
Extractive and utility supply industries	1 in 20000	50
Agriculture, hunting, forestry and fishing (not sea fishing	1 in 17200	58
Manufacture of basic metals and fabricated metal products	1 in 34000	29
Manufacturing industry	1 in 77000	13
Manufacture of electrical and optical equipment	1 in 500000	2
Service industry	1 in 333000	3

5.5.3 What it includes

5.5.3.1 Methodology

Formal Safety Assessments consist of a five step risk assessment process that is outlined below. The process also can include human tasks and these have been included where they are appropriate.


Formal Safety Assessment Methodology
Tasks Required to Incorporate Human Reliability Analysis
Step 1
Hazard Identification
Human Related Hazards
High Level Task Analysis
Preliminary Descriptive of Outcome
Step 2
Risk Analysis
Detailed Task Analysis for Critical Tasks
Human Error Analysis
Human Error Quantification
Step 3
Risk Control Options
Risk Control Options for Human Element
Step 4
Cost Benefit Analysis
Step 5
Recommendations for Decision Making

Step 1. Identification of hazards (a list of all relevant accident scenarios with potential causes and outcomes); e.g. structured group reviews, functional failures, historic reviews etc.

Step 2. Risk Analysis (evaluation of risk factors); a detailed investigation of the causes and consequences of hazards identified in Step 1. Using e.g. fault trees, event trees, conceptual risk models

Step 3. Risk control options (devising regulatory measures to control and reduce the identified risks). This involves ranking the risks and then determining the most appropriate Risk Control Measures (RCM) to apply.

Step 4. Cost benefit assessment (determining cost effectiveness of each risk control option);

Step 5. Recommendations for decision-making (information about the hazards, their associated risks and the cost effectiveness of alternative risk control options is provided). This includes comparison with the risk criteria

Figure 15: The FSA Methodology

Within the FSA, individual fatality risk criteria are used when reviewing the overall safety of the vessel. If residual risks are lower than the tolerable estimates, but above negligible a CBA process should be used to evaluate which if any risk reducing measurers should be implemented.

Figure 16 below shows how the historical performance of the annual fatality risk for crew for different types of vessel is against the intolerable and negligible risk described above. As can be seen, the historical performance puts current vessels in the ALARP region. When this occurs then a cost-benefit analysis should be carried out to determine if additional risk reduction measures should be carried out.

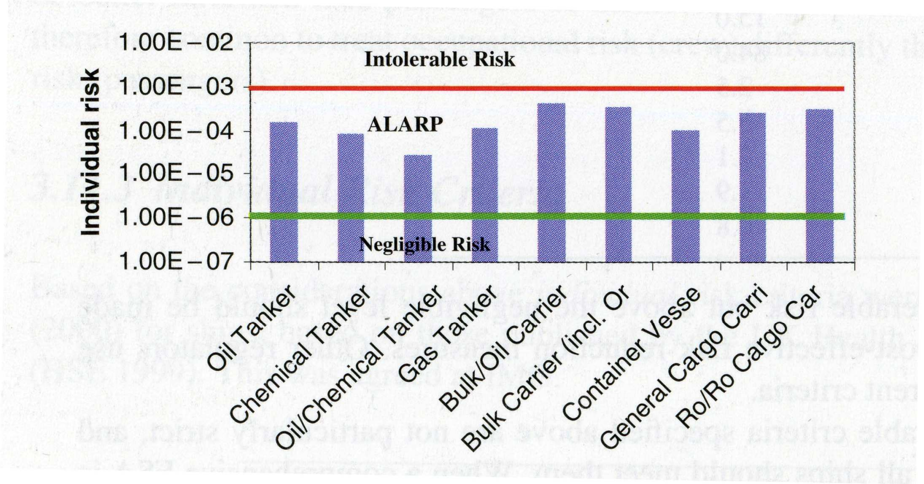


Figure 16: Individual annual fatality risk for crew of different ship types (Data from 1978-1998), Reproduced from [22].

5.5.3.2 Cost Benefit Analysis

The cost benefit analysis is the second type of criteria that the FSA includes. It can be used primarily as a screen tool to reduce the number of options identified in Step 3 of the methodology such that only relevant options are recommended in Step 5, the decision making process.

Costs should be expressed in terms of life cycle costs and may include initial, operating, training, inspection, maintenance, certification, decommission etc. Benefits may include reductions in fatalities, injuries, casualties, environmental damage and clean-up, indemnity of third party liabilities, etc. and an increase in the average life of ships.

In the table below, the actual cost of the risk reduction measures considered is described. In general the accepted cost of averting a fatality is in the region US$1.5m - US$5m. Full details of CBA Values used in FSA are included in [22].

Table 14: Cost of averting fatalities in actual decision

Decision	Decision Maker	Value (US$ millions)
Strengthening bulkheads on existing bulk carriers	IACS and IMO	> 1.5
3 bulkheads on car decks	IMO	< 5
Collision avoidance training	Owner	> 0.7
Extra deck officer	IMO	< 5.5

5.5.3.3 Human Reliability Analysis (HRA)

The formal safety assessment uses QRA to assess the frequency of system failures as part of the design process or ongoing operations management. In order to produce valid results it is necessary to assess the contribution of the human element to system failure. The accepted way of incorporating the human element into QRA and FSA studies is through the use of human reliability analysis (HRA).

HRA is primarily used in the hazard identification (step 1), and risk analysis (step 2) parts of the FSA as shown in the overall FSA structure above. The key areas are

1. Identification of key human tasks consistent with step 1; this can be done using a Hazard and Operability (HazOp) study or a Failure Mode and Effects Analysis (FEMA), however in addition a high-level functional task analysis can be carried out.
2. Risk assessment, including a detailed task analysis, human error analysis and human reliability quantification consistent with step 2. This task analysis would be at a more detailed level when compared with that in step 1, and this would then be followed by a human error analysis. The potential errors are then classified in terms of:
   a. the supposed cause of the human error;
   b. the potential for error-recovery, either by the operator or by another person (this includes consideration of whether a single human error can result in undesired consequences); and
   c. the potential consequences of the error.

   If these then require full quantification then a technique is needed for determining the probability of human error (HEP). A number of tools exist for this, most of which have transferred from the nuclear industry, these include: Absolute Probability Judgement (APJ), Technique for Human Error Rate Prediction (THERP) and Human Error Assessment and Reduction Technique (HEART).
3. Risk control options consistent with step 3. These risk control options can be approached in exactly the same way as for other risk control options, i.e. the measures can:
   a. reduce the frequency of failure;
   b. mitigate the effects of failure;
   c. alleviate the circumstances in which failures occur; and
   d. mitigate the consequence of accidents.

Further details of how the FSA method can include HRA can be found in Appendix 1 of [19].

5.5.4 What it Excludes

The FSA is applied to generic designs, and then sets rules for those generic designs, so it does not include and specific low level criteria. As can be seen in the examples of risk control options described in Table 14 the options identified are typically of the high-level type but can include both technical systems or human performance aspects.

5.5.5 Summary and Comparison with ERA's Study Objectives

1. The identification of RAC at a technical level and operational/procedural level.

The International Maritime Organisation applies Formal Safety Assessment using two types of criteria, individual risk targets (for crew, passengers and the public) both as maximum frequencies, and as target frequencies. These individual risk targets are related to those found in the highest risk industries. In addition, once the risk is in the ALARP range, financial criteria are used to determine if additional risk reduction measures are appropriate.

The FSA can include Human Reliability Analysis, either to determine human induced hazards and recovery mechanisms or to support quantitative analysis.

2. Are human reliability or semi quantitative techniques such as the SILs or other qualitative rules used to accept human driven actions that allow assessment and acceptance of the systems?

Several HRA techniques can be used to provide data on the performance or crew both in normal and emergency conditions. These include the THERP and HEART methods. Alternatively and APJ technique can be used.

3. *The minimum requirements for performing safety critical tasks should be analysed by studying relevant legislation, guidance or safety management systems. These may also range from quantitative values for the human reliability to description of principles on education or redundancy through check by different people.*

As FSA applied to generic ship designs, rather than actual systems then the human modelling is necessarily generic; risk reduction measures can include improvement in crew training or number of crew, however the general crew performance is less relevant to this type of assessment.

5.5.5.1 Concluding Remarks

We conclude by asking ***could the FSA (or similar) be used in the context of assigning RAC?*** The answer to this question is that whilst the values are interesting the scope is different from that required by the ERA.

Individual risk targets make sense for generic ship designs. The ship can be seen as a relatively closed system, and the targets apply to passengers and crew. For rail the systems are more interactive and system reliability can be considered to be more important.

The FSA makes use of the ALARP principle to take criteria beyond the maximum tolerable risk towards acceptable risk and evaluates the acceptability of addition risk reduction measures using a Cost-Benefit Analysis method. This could be an area ERA could consider for further study as it ensures additional risk reduction measures which only have a marginal addition cost are taken forward for consideration.

6.0 Conclusions

6.1 Organisations using RAC and their Type

We have identified that harmonised Risk Acceptance Criteria (RAC) are used in the aviation, nuclear, maritime sectors and also that pan-industry RAC are defined in a number of Member States (see Table 1 and Appendix I for more details).

We note the existence of two options for setting RAC, as follows:

1. RAC that are "evidence" based. Such RAC are based on historical evidence derived from an analysis of previous safety performance (possibly with an improvement factor built in).
2. RAC that are aspirational or "technology-driving". Such RAC are normally set regardless of whether experience indicates they are currently attainable.

The results of our research indicate that evidence based goals are the norm when setting industry RAC. In fact all the industry schemes reported here (aviation, maritime) as well as the UK national scheme, are all set based on an analysis of past performance. In this respect we note that the ERA has specified evidence based goals in terms of the National Reference Values (NRVs). Such evidence based schemes are usually accompanied by a requirement to demonstrate that risks have been managed to a level where they are insignificant, or to a level where the benefits of further risk reduction are outweighed by the resources needed to implement them.

The exception to this rule applies in The Netherlands where aspriational RAC are set. These targets are set regardless of whether past performance indicates they can be achieved. It is the norm that achievement of such targets is the end of the matter, and that there is little requirement for further risk reduction measures to considered.

6.2 Derivation and Apportionment of RAC

We note that, for the schemes presented above, RAC are usually defined at a high level (representing RAC for the entire operation or undertaking, or possibly at a major hazard level).

Where a low level or *de minimis* criterion is applied (specifically aviation) this has been achieved through an apportionment technique. The apportionment techniques used was based on engineering judgement rather than a rigorous mathematical process.

6.3 Demonstrating Compliance with RAC

Bow-tie QRA models are frequently used as the preferred means of assessment (e.g. the Safety Risk Model (SRM), the Accidental Risk Assessment Methodology (ARAMIS), the Integrated Risk Picture (IRP) etc) and demonstrating compliance with RAC. Within these methods human reliability is usually included explicitly.

A number of variants of Safety Integrity Level (SIL) based techniques are used within industry for various purposes. These include the Level of Confidence assessment with the ARAMIS approach. This includes: a method that can be used to justify the setting of a Level of Confidence; a method for assessing the required Level of Confidence that a safety barrier must meet to achieve a certain safety performance level; a method for determining whether a design meets a Level of Confidence requirement.

We also summarise an approach within ARAMIS that seeks to identify the impact of safety management systems and of an organisation's safety culture has on safety performance. This is achieved through an audit process which is then used as an input to the establishment of safety barrier effectiveness.

We have identified no methods or examples that have led to the setting of RAC at the operational level (as would complement the technical system criteria described at Section 3.2). Within the Eurocontrol Safety Assessment Methodology however a process is described to cover the design guidelines for procedures. In particular, it discusses a method for establishing a risk based approach to the level of development and checking a procedure must be subject to in order to meet a safety requirement.

Other techniques, such as the use of a risk matrix in the Great Britain safety framework, provide alternative means of achieving the goals of RAC apportionment and of ensuring that the contribution of individual hazards does not compromise the overall system safety target.

6.4 Consensual and Other Railway Standards

We provide specific references as Section 7 of this report.

Additionally we have referred to SIL and software assurance level based techniques variously through this report, and the concepts underpinning the use of these appears in many industries, including railway, either in their standard form or modified for a particular application. The underpinning document is:

- IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems.

Additional railway specific standards include:

- EN 50126: Railway Applications. The specification and demonstration of reliability, availability and maintainability.
- EN 50128: Railway Applications. Communications, signalling and processing systems. Software for railway control and protection systems.
- EN 50129: Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling.

7.0 References

01 DNV, ‘Inception Report – Risk Acceptance Criteria’, Report No: 24127328/01, Rev 1 dated 10 September 2009.

02 DNV, ‘Scoping Report – Risk Acceptance Criteria for Technical Systems and Operational Procedures’, Report No: 24127328/02, Rev 1 dated 30 October 2009.

03 Official Journal of the European Union, DIRECTIVE 2004/49/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ‘The Railway Safety Directive’, of 29 April 2004.

04 ERA, ‘CSM Working Group Risk Acceptance Criteria’, Report: Risk Acceptance Criteria, Rev 1.0, dated April 2009.

05 ERA, ‘RAC in other industries - Kick off meeting with DNV’, Lille, 28 July 2009

06 EASA decision no. 2003/2/RM of the executive director of the agency of 17 October 2003 on certification specifications, including airworthiness codes and acceptable means of compliance, for large aeroplanes (CS-25); EASA Acceptable Means of Compliance (AMC) 25.1309-1, System Design and Analysis.

07 ARP, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, Society of Automotive Engineers, ARP 4761, December 1996

08 EUROCONTROL ESARR ADVISORY MATERIAL/ACCEPTABLE MEANS OF COMPLIANCE (EAM/AMC), EAM 4 / AMC ACCEPTABLE MEANS OF COMPLIANCE WITH ESARR 4, Edition 3.0, 10/08/04

09 EUROCONTROL SAM Electronic v2.1, 2006

10 Council of the European Union, ‘The control of major-accident hazards involving dangerous substances’ Seveso II Directive 96/82/EC, dated 9 December 1996

11 The European Commission Community Research ’Accidental Risk Assessment Methodology for Industries in the Context of the Seveso II Directive’, Contract No: EVG1 – CT – 2001 – 00036, dated December 2004.

12 ARAMIS Audit Manual, Version 1.2; dated 9 / 3 / 2004 (http://mahb.jrc.it/index.php?id=447)

13 ARAMIS D1C - APPENDIX 7, Frequencies and probabilities data, July 2004 (http://mahb.jrc.it/index.php?id=447)

14 ARAMIS D1C – APPENDIX 9, Assessment of the performances of safety barriers, 9 July 2004 (http://mahb.jrc.it/index.php?id=447)

15 ARAMIS D1C – APPENDIX 14, The Risk Graph, July 2004 (http://mahb.jrc.it/index.php?id=447)

16 Rail Safety and Standards Board, ‘The Railway Strategic Safety Plan’ 2009 - 2014

17 The Railways and Other Guided Transport Systems (Safety) Regulations 2006, ISBN 0110743075

18 The Health and Safety Executive, ‘The development of a fatigue / risk index for shiftworkers’, RESEARCH REPORT 446 dated 2006

19 International Maritime Organisation, Guidelines for Formal Safety Assessment (FSA) for use in the IMO Rule Making Process, T1/3.02, T5/1.01, 05/04/02.

20 Health and Safety Executive, ‘Reducing Risks, Protecting People’, HSE Books, ISBN 0 7176 2151 0, first published 2001

21 Risk Evaluation Criteria, SAFEDOR EC 6FP Programme, Design, Operation and Regulation for Safety, Rolf Skjong, Erik Vanem, Oyvind Endresen

22 Risk Based Ship Design, Methods Tools and Applications, Apostolos D Papanikolaou (Ed), ISBN: 978-3-540-89041-6

23 EUROCONTROL Safety Regulatory Requirement (ESARR) 4: Risk Assessment and Mitigation in Air Traffic Management, Edition 1.0, 05/04/2001.

24 EUROCONTROL Air Navigation System Safety Assessment Methodology (SAM), SAF.ET1.ST03.1000-MAN-01, v2.0, 30/04/2004.

25 Official Journal of the European Union, COMMISSION REGULATION (EC) No 2096/2005 of 20 December 2005 laying down common requirements for the provision of air navigation services, L335/13

26 ICAO Annex 11 to the Convention on International Civil Aviation, Air Traffic Services, Air Traffic Control Service, Flight Information Service, Alerting Service, Thirteenth Edition.

27 INTERNATIONAL STANDARD ISO 17776 Petroleum and natural gas industries — Offshore production installations — Guidelines on tools and techniques for hazard identification and risk assessment, first edition 15/10/2005.

28 International Code of Safety for High-Speed Craft (HSC Code) (resolution MSC.36 (63), which was developed following a revision of the Code of Safety of Dynamically Supported Craft (resolution A.373(X)).

29 Health and Safety Executive, 'The Health and Safety At Work Act 1974', ISBN 0 11 141439 X, dated 1974.

30 Health and Safety Executive, 'Reducing Risks, Protecting People', HSE Books, ISBN 0 7176 2151 0, first published 2001

31 Ale BJM, 'Tolerable or Acceptable: A Comparison of Risk Regulation in the United Kingdom and the Netherlands' Risk Analysis, Vol 25 No 2 2005.

32 EUROCAE (EURopean Organisation for Civil Aviation Equipment), ED-125, Process for Deriving Risk Classification Scheme and Specifying Safety Objectives in ATM "in compliance" with ESARR 4, Version 6 (proposed issue).

33 European Committee for Electrotechnical Standardization (CENELEC), EN 50128, Railway applications, Communication, signalling and processing systems, software for railway control ad protection systems, 2001

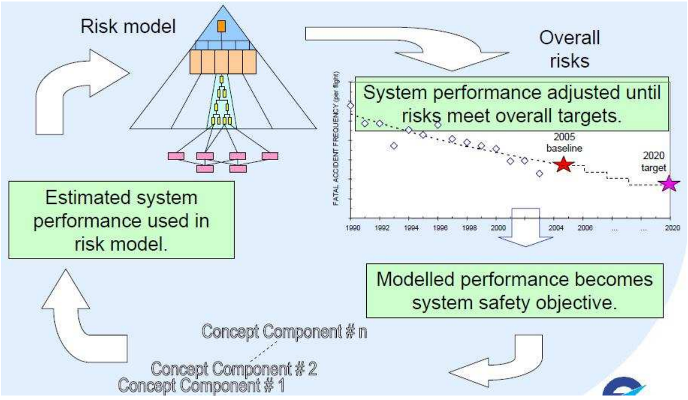
34 International Association of Classification Societies (IACS), Classification societies, What, Why and How? November 2009, www.iacs.org.uk.

Appendix I Scoping Study Summary Tables

Table 15 Summary of RAC in Aviation Air Traffic Management

Scheme Owner / Name:	***EUROCONTROL Safety Regulatory Requirement (ESARR) 4: Risk Assessment and Mitigation in Air Traffic Management [23]*** ***Eurocontrol Safety Assessment Methodology (ESAM) [24]***
Scheme Coverage:	Geographical scope includes all 44 European Civil Aviation Council (ECAC) States.
Are RAC Used?	***Yes***
If RAC Used:	***Type***: High level target. A maximum tolerable probability of 1.55*10^{-8} per flight hour of an Air Traffic Management direct contribution to an accident. Derived from a historical analysis of the frequency of ATM contribution to accidents and an analysis that the absolute frequency should not increase (despite increased traffic growth).
	Form: Target safety level
Brief Description:	The risk target for ATM direct contribution to an accident of 1.55 * 10^{-8} per flight hour is defined in the ESARR 4 requirements for the provision of air traffic services[2]. These requirements apply to ECAC member states. States are free to develop their own risk assessment methodology that is compatible with this requirement. The European Union Commission Regulation CR 2096/2005 [25] also adopts all mandatory provisions of ESARR 4, which includes the maximum tolerable probability. The common requirement also requires a risk assessment to be carried out against this system; however the precise form of this risk assessment is not specified. Several European States have developed risk assessment methodologies that are compatible with this requirement. One methodology that is generic is the Safety Assessment Methodology (SAM) that has been developed by EUROCONTROL. A key issue for this methodology is the apportionment of the risk target to individual systems or elements in order to assess a new or changed system. This is particularly challenging when there are significant changes to the system, e.g. for the future ATM system being developed as part of the Single European Sky ATM Research programme (SESAR). For this Eurocontrol developed the Integrated Risk Picture. This is a holistic top-down model of the ATM contribution to accident risk. It can be used to enable systematic apportionment of safety targets and consistency of the top level claims in safety cases, see below.

[2] EUROCONTROL has also been tasked with re-developing this risk classification scheme including maximum tolerable frequencies for lower severity events, this work is currently ongoing and the value of the top level target may change given more recent data.


Risk model
Overall risks
System performance adjusted until risks meet overall targets.
FATAL ACCIDENT FREQUENCY (per flight)
2005 baseline
2020 target
1990
1992
1994
1996
1998
2000
2004
2006
...
...
2020
Estimated system performance used in risk model.
Modelled performance becomes system safety objective.
Concept Component # n
Concept Component # 2
Concept Component # 1

A relatively new development within the ESAM methodology has been the introduction of Procedure Assurance Levels (PALs). These fit within the previous risk criteria but can be used when a procedural failure could lead to a hazard in the system under investigation. The probability of the procedure failure leading to a certain severity of consequence is evaluated, and then the required PAL is determined from the table below.

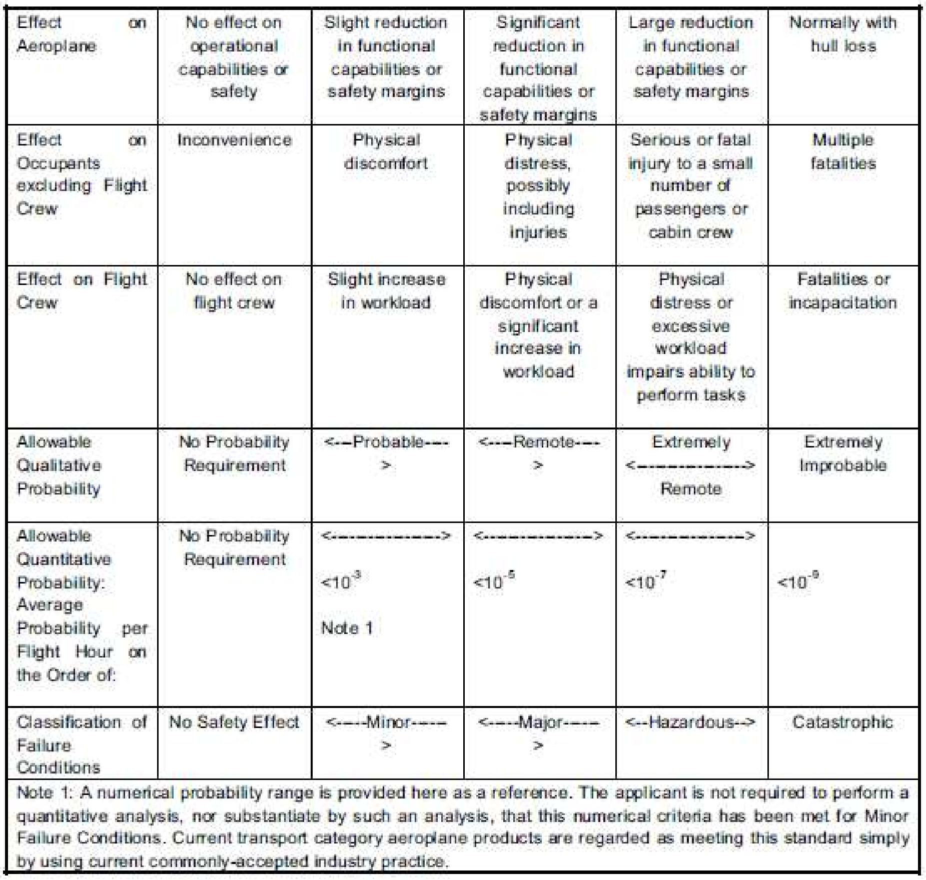
		Severity			
		1	2	3	4
Probability	Very possible	PAL1	PAL2	PAL3	PAL4
	Possible	PAL2	PAL3	PAL4	PAL4
	Very unlikely	PAL3	PAL3	PAL4	PAL4
	Extremely unlikely	PAL4	PAL4	PAL4	PAL4

These different PALs have defined requirements in terms of procedure development, testing and implementation in an analogous manner to Software Assurance Levels.

Scheme maturity:	Since 2005 as part of the common requirements, since 2001 as part of the EUROCONTROL Safety Regulatory Requirements (ESARR 4).

Table 16 Summary of RAC in Aviation Aircraft Design

Scheme Owner / Name:	***European Aviation Safety Agency (EASA), EASA AMC 25*** [06] (analogous schemes are used in the US).
Scheme Coverage:	All 31 EASA Member States.
Are RAC Used?	***Yes***
If RAC Used:	***Type**:* System level targets A maximum average probability of ***10^{-9} per flight hour*** that an individual failure will lead to a catastrophic accident. Additional targets against hazardous (10^{-7} per flight hour) and major (10^{-5} per flight hour) failure conditions. The values are chosen [06] following historical analysis of the aircraft system contribution to accidents and apportioning this equally across an arbitrary 100 potential failure conditions.
	Form: Tolerable probabilities of Catastrophic, Hazardous and Major consequences
Brief Description:	System safety requirements for aircraft design are specified in Europe by EASA and in the United States by the Federal Aviation Administration. The requirements specify a limit of ***10^{-9} per flight hour*** that an individual failure will lead to a catastrophic accident. If this target cannot be met, there is also an alternative requirement that ***no single failure will result in a catastrophic failure condition***, and that the ***sum of all failure conditions should be less than 10^{-7} per flight hour***.



Effect on Aeroplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants excluding Flight Crew	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a small number of passengers or cabin crew	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatalities or incapacitation
Allowable Qualitative Probability	No Probability Requirement	<---Probable---->	<----Remote---->	Extremely <-------------> Remote	Extremely Improbable
Allowable Quantitative Probability: Average Probability per Flight Hour on the Order of:	No Probability Requirement	<-------------> $<10^{-3}$ Note 1	<-------------> $<10^{-5}$	<-------------> $<10^{-7}$	$<10^{-9}$
Classification of Failure Conditions	No Safety Effect	<----Minor---->	<----Major---->	<--Hazardous-->	Catastrophic

Note 1: A numerical probability range is provided here as a reference. The applicant is not required to perform a quantitative analysis, nor substantiate by such an analysis, that this numerical criteria has been met for Minor Failure Conditions. Current transport category aeroplane products are regarded as meeting this standard simply by using current commonly-accepted industry practice.

Table reproduced from EASA AMC 25.1309 [06].

These risk criteria are then used inside a comprehensive safety assessment

	methodology linked to the aircraft and system development cycle. This four stage safety assessment process encompasses: 1. Aircraft and System Functional Hazard Assessment. 2. Aircraft and System Preliminary System Safety Assessments. 3. System Safety Assessments. 4. Common Cause Analysis.
Scheme maturity:	Scheme used for 20 years across Europe and the USA covering aircraft certification requirements, some slight updates and differences between systems.
Comments:	The version applicable in the USA is published by the Federal Aviation Administration (FAA) and refers to requirements of the Federal Aviation Regulations (FAR) 25.1309(b). The acceptable means of compliance are defined in FAA Advisory Circular, AC 25.1309-1A, System Design and Analysis (6/21/1988).

Table 17 Summary of RAC in Aviation against Mid Air Collision

Scheme Owner / Name:	ICAO (International Civil Aviation Organisation; a specialised agency of the United Nations). ***ICAO Mid-Air Collision (MAC) Risk Target [26]***
Scheme Coverage:	The ICAO contracting States number 190 with worldwide coverage including for example all European States, USA, Japan and China. Full details are available on the ICAO website.
Are RAC Used?	***Yes***
If RAC Used:	***Type:*** High level target A target frequency of ***5 * 10^{-9} fatal accidents per flight hour*** per dimension (i.e. vertical or two horizontal dimensions). A mid-air collision accident involves two aircraft. Derived from a historical analysis of the frequency of mid-air collisions, and an extrapolation for the trend in reduced overall accident rate.
	Form: Target safety level
Brief Description:	The ICAO MAC risk target does not come with an associated risk assessment methodology, instead it is a target used in specific relevant cases within other methodologies (e.g. the ESAM). This criterion involves all causes of Mid-Air Collisions including technical systems and human factors. The target still requires apportioning to systems, e.g. in the safety case developed by EUROCONTROL to support the Reduction of Vertical Separation Minima from 2000 ft to 1000 ft then up to 50% of this target was assigned to technical systems (altimeters etc) and the remaining risk to other errors including human error.
Scheme maturity:	Present RAC adopted in 1995, although similar criteria have been used since the 1960's.
Comment:	Other specific targets have been published by ICAO e.g. for the risk of a catastrophic accident during a precision approach. The RAC value would again be used within other schemes, either EUROCONTROL or individual State schemes.

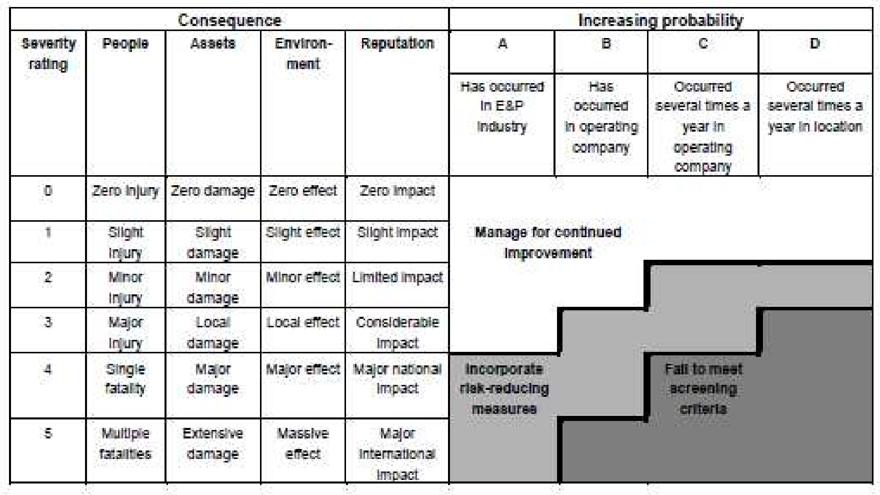
Table 18 Summary of RAC in the Nuclear Sector

Scheme Owner / Name:	***European Council EURATOM 96/29*** *"basic safety standards for the protection of the health of workers and the general public against the dangers arising from ionizing radiation"*
Scheme Coverage:	***European Union Member States***
Are RAC Used?	***Yes***
If RAC Used:	***Type:*** EURATOM 96/29 specifies ***maximum dosage*** targets for exposed workers and other affected groups. Member States may specify alternative maximum dosage limits in some cases. There is also a requirement that each Member State shall take reasonable steps to "*ensure that the contribution to the exposure of the population as a whole from practices is kept as low as reasonably achievable, economic and social factors being taken into account.*"
	Form: Cumulative dosage level over a stated period of time. Exposure to ionizing radiation may lead to a health detriment over time, and the possibility of death. Exposure levels are specified to reduce the risk of such health detriments to acceptable levels.
Brief Description:	Individual exposure levels are defined for: exposed workers; public at large; special groups. For exposed workers several maximum exposure levels are defined, an example of which is provided in the text above. In addition to overall dosage exposures, specific body areas are identified separately (eyes, hands, feet etc). For members of the public and the general population, lower maximum exposure levels are defined with a requirement that these are kept as low as reasonably achievable. Additionally, certain specific groups (such as persons under the age of 18, pregnant women) are given special consideration. Specific guidance is provided concerning how dosage levels are calculated so that a common approach is applied across Member States. Any further requirement for risk assessment is contained in Member States own guidance. We note that the Nuclear sector is a prime mover in developing and using Human Reliability Analysis prediction and calculation techniques. A number of tools are available for this purpose. The Standardised Plant Analysis Risk – Human Reliability Analysis (SPAR-H) is a recent development in this field. SPAR-H was developed by the US Nuclear Regulatory Commission in 2005 following a review of a number of alternative techniques. The purpose of SPAR-H is to generate human reliability estimates for use in risk assessments and considers the task being undertaken and shaping factors which may include training, time limitations etc.
Scheme maturity:	EURATOM 96/29 was required to be enforced by Member States on or before 13 May 2000.

Table 19 Summary of RAC in the Chemical Sector

Scheme Owner / Name:	***European Council DIRECTIVE 96/82/EC*** *on the control of major-accident hazards involving dangerous substances and associated guidance*
Scheme Coverage:	***European Union Member States***
Are RAC Used?	***No***
If RAC Used:	***Type:*** Not applicable
	Form: Not applicable
Brief Description:	The Safety Report and Land Use Planning Guidance require that a risk assessment is undertaken, and a general framework is proposed. To support this, the European Commission Community Research Programme has completed research into a methodology called ARAMIS. This is an integrated risk assessment process based on the: 1. Identification of major accident hazards. 2. Identification of the safety barriers and assessment of their performance. 3. Evaluation of safety management efficiency to barrier reliability. 4. Identification of Reference Accident Scenarios. 5. Assessment and mapping of the risk severity of reference scenarios. 6. Evaluation and mapping of the vulnerability of the plant's surroundings. Its purpose is to provide the basis for a common approach to risk assessment using standard tools, techniques and data, thus producing more consistent results across the industry. Step 1 (major hazards identification) uses fault and event tree analysis techniques. The process provides a methodology for identifying those equipments which are the most likely to lead to major hazards leading to the quantification of risks. Step 2 (safety barriers) provides a process for identifying safety barriers that may reduce the likelihood or consequence of the identified major hazards; the effectiveness of the barrier is assessed via ARAMIS. Step 3 (safety management) provides a structured process for assessing the safety management system and safety culture of an organisation and the influence this has on the performance of the safety barriers identified in step 2. It is implemented through a questionnaire based approach. Step 4 (scenarios) seeks to identify the risks that are to be further assessed. A risk matrix is used to guide this selection, supported by guidelines for estimating the frequency and consequence of the scenarios. Steps 1 to 4 are common to most major hazard activities. Step 5 (assessment and mapping) and step 6 (vulnerability) involve the development of risk contours and then overlaying the risk contours onto the sites local surroundings. These assessments are specific to this industry and are thus not addressed here. Within the process, ARAMIS has specified human error performance rates (as a probability of failure on demand). It also uses the concepts of Safety Integrity Levels as defined in IEC 61508 and IEC 61511 to define the effectiveness of safety barriers.
Scheme maturity:	The Seveso Directive was first adopted in 1982.

Table 20 Summary of RAC in the Offshore Sector

Scheme Owner / Name:	***International Standards Organisation (ISO) 17776 Petroleum and natural gas industries – Offshore production installations – Guidelines on tools and techniques for hazard Identification and risk assessment [27]***
Scheme Coverage:	***Worldwide***
Are RAC Used?	***No***
If RAC Used:	***Type:*** Not applicable
	Form: Not applicable
Brief Description:	ISO 17776 defines a generic risk assessment methodology with the typical steps of hazard identification, risk evaluation and the setting of functional requirements. An example risk evaluation matrix is included in the standard, but it is made clear that matrices should be developed specific to the activity under consideration. **Table A.1 — Example of risk matrix and consequences that may be considered** 
Scheme maturity:	ISO 17776 was published October 2000

Consequence					Increasing probability			
Severity rating	**People**	**Assets**	**Environment**	**Reputation**	A	B	C	D
					Has occurred in E&P industry	Has occurred in operating company	Occurred several times a year in operating company	Occurred several times a year in location
0	Zero injury	Zero damage	Zero effect	Zero impact				
1	Slight injury	Slight damage	Slight effect	Slight impact	**Manage for continued improvement**			
2	Minor injury	Minor damage	Minor effect	Limited impact				
3	Major injury	Local damage	Local effect	Considerable impact				
4	Single fatality	Major damage	Major effect	Major national impact	**Incorporate risk-reducing measures**		**Fail to meet screening criteria**	
5	Multiple fatalities	Extensive damage	Massive effect	Major international impact				

Table 21 Summary of RAC in the Maritime Sector for Formal Safety Assessment

Scheme Owner / Name:	IMO (International Maritime Organisation), a specialised agency of the United Nations. ***IMO Formal Safety Assessment (FSA) [19]***
Scheme Coverage:	The membership of the IMO is 169 member states and three associate members with worldwide coverage. A full list is available on the IMO website.
Are RAC Used?	***Yes*** but values not defined in methodology
If RAC Used:	***Type:*** Global individual and societal risk targets. Maximum tolerable annual risk of fatality **for crew members of 10^{-3}** and for **passengers/public of 10^{-4}** is specified. Beyond this tolerable criterion, a **cost-benefit analysis (CBA)** on additional risk reducing measurers is conducted.
	Form: Tolerable individual fatality risk; injuries are included in the cost-benefit analysis
Brief Description:	FSA is a structured and systematic methodology, aimed at enhancing maritime safety, including protection of life, health, the marine environment and property through the use of risk analysis and cost benefit assessment. FSA is applied to generic ship designs, not individual ships. Risk reduction measures, if deemed by the FSA as needed are implemented as prescriptive rules for that ship type. This means there is no need for any low level risk acceptance criteria. The FSA consists of five steps: 1. Identification of hazards (a list of all relevant accident scenarios with potential causes and outcomes); 2. Assessment of risks (evaluation of risk factors); 3. Risk control options (devising regulatory measures to control and reduce the identified risks); 4. Cost benefit assessment (determining cost effectiveness of each risk control option); and 5. Recommendations for decision-making (information about the hazards, their associated risks and the cost effectiveness of alternative risk control options is provided). Criteria are not formally defined within the methodology however individual risk criteria have subsequently been agreed. These are defined per ship-year: • Maximum tolerable fatality risk for crew members ***10^{-3} annually*** • Maximum tolerable fatality risk for passengers or public ***10^{-4} annually*** • Negligible fatality risk ***10^{-6} annually*** These targets are not particularly strict, and instead when considering a comprehensive FSA on new ships a stronger target should be used: • Maximum tolerable fatality risk for ***crew members 10^{-4} annually*** • Maximum tolerable fatality risk for ***passengers or public 10^{-5} annually*** Societal risk should also be considered, and this is done through the use of F-N curves. If residual risks are lower than the tolerable estimates, but above negligible a CBA process should be used to evaluate which if any risk reducing measurers should be implemented. From recent FSAs carried out the cost of averting a fatality is in the region US$1.5m to US$5m. The FSA scheme also includes humans within the assessment through use of a human reliability analysis, task analysis and the allocation of human error probabilities.
Scheme maturity:	Started in the early 1990's, but approved for use in the IMO rule-making process in 2002.

Table 22 Summary of RAC in the Maritime Sector for High Speed Craft

Scheme Owner / Name:	***International Code for High Speed Craft IMO*** [28] (International Maritime Organisation), a specialised agency of the United Nations.
Scheme Coverage:	The membership of the IMO is 169 member states and three associate members with worldwide coverage. A full list is available on the IMO website.
Are RAC Used?	***Yes***
If RAC Used:	**Type:** System level target Acceptance criteria that a failure mode that has a catastrophic effect should only have a probability of occurrence that is extremely improbable (less than 10^{-9} per hour). Additional criteria are defines for hazardous and minor effects.
	Form: Tolerable probabilities of Catastrophic, Hazardous and Minor consequences.
Brief Description:	The international code of safety for high speed craft applies to amongst others, air cushion vehicles (such as hovercraft) and hydrofoil boats. The regulation includes a requirement for a Failure Modes and Effects Analysis (FMEA) of all new designs of high speed craft on international voyages. Acceptance criteria for failure modes are defined in an analogous manner to those used by the European Aviation Safety Agency (EASA) for aircraft design, namely; Minor effect Reasonably probable Hazardous effect Extremely remote Catastrophic effect Extremely improbable The code goes on to state that a failure mode leading to a catastrophic effect should be guarded against by system or equipment redundancy unless the probability meets the extremely improbable criteria. The effects are defined in terms of catastrophic meaning multiple fatalities or loss of vessel; hazardous meaning serious or fatal injuries to a small number of occupants and major meaning discomfort or minor injuries. The probabilities are given further definition in terms of risk per hour or per journey and a descriptive definition. Extremely improbable is further defined as a failure condition that is at worst ***10^{-9}***, with extremely remote in the ***10^{-9}*** - ***10^{-7}*** range and reasonably probable in the range ***10^{-5}*** to ***10^{-3}***.
Scheme maturity:	The code on high speed craft was passed in 1995. The code was updated in 2000.

Table 23 Summary of RAC in the Road Transport (Dangerous Goods) Sector

<table>
<tr><td><b>Scheme Owner / Name:</b></td><td><b><i>United Nations Economic Commission for Europe (Committee on Inland Transport)</i></b> <i>- agreement Concerning the International Carriage of Dangerous Goods by Road (ADR 2009)</i></td></tr>
<tr><td><b>Scheme Coverage:</b></td><td><b><i>European Union Member States (and others)</i></b></td></tr>
<tr><td><b>Are RAC Used?</b></td><td><b><i>No</i></b></td></tr>
<tr><td rowspan="2"><b>If RAC Used:</b></td><td><b><i>Type:</i></b> Not applicable</td></tr>
<tr><td><b><i>Form:</i></b> Not applicable</td></tr>
<tr><td><b>Brief Description:</b></td><td>ADR 2009 provides prescriptive requirements for the carriage of dangerous goods by road (with tunnels receiving particular attention). These include requirement for the classification of dangerous goods, as follows:
<table>
<tr><th>Tunnel Category</th><th>Restriction</th></tr>
<tr><td>A</td><td>No restrictions</td></tr>
<tr><td>B</td><td>Restriction for dangerous goods which may lead to a very large explosion</td></tr>
<tr><td>C</td><td>Restriction for dangerous goods which may lead to a very large explosion a large explosion or a large toxic release of dangerous goods restricted in tunnel category B</td></tr>
<tr><td>D</td><td>Restriction for dangerous goods which may lead to a very large explosion to a large explosion to a large toxic release or to a large fire dangerous goods restricted in tunnel category C</td></tr>
<tr><td>E</td><td>Restriction for all dangerous goods other than UN Nos. 2919, 3291, 3331, 3359 and 3373</td></tr>
</table>
<p>The categorisation given to each consignment leads to a set of conditions that must be met in order that (in this example) the tunnel can be used to transport the dangerous goods. Within the context of this system, the term risk is used in the descriptive sense.</p>
<p>It is of interest to note that ADR was updated to include a new classification system recommended following research completed by the Organisation for Economic Co-operation and Development. The work also proposed a risk model and decision support model be created, but this was <b><i>not adopted</i></b>.</p></td></tr>
<tr><td><b>Scheme maturity:</b></td><td>First implemented during 1957</td></tr>
</table>

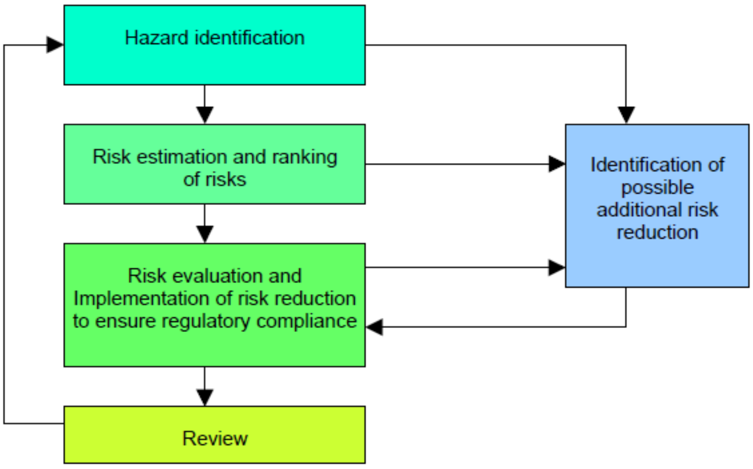
Table 24 Summary of RAC in GB

Scheme Owner / Name:	***Health and Safety Executive (HSE), the Health and Safety At Work Act 1974 (the HSW Act) [29]***
Scheme Coverage:	***United Kingdom (all industries)***
Are RAC Used?	***Yes***
If RAC Used:	***Type:*** The HSE specifies ***high/global level boundaries*** [30] that define regions on a risk acceptance graph. These boundaries relate to individual risk. The concept of societal concern is also addressed again in ***high level/global terms***. The targets were selected by the HSE based on its experience in collecting and analysing UK accident statistics. The RAC and the framework were subject to a period of consultation prior to finalisation.
	Form: Risks are specified in terms of possibility of death per annum. An example of an individual risk criteria boundary is provided in the text above. For societal risks, the HSE (using as an example a major chemical site near a housing estate) state the ***risk of an accident causing the death of 50 people or more in a single event should be regarded as intolerable if the frequency is estimated to be more than one in five thousand per annum***.
Brief Description	Brief details of the application of the HSW Act and associated guidance are provided by industry sector below. In general an undertaking covered by the HSW Act is required to complete a risk assessment. If that risk assessment shows that the annual risk of death is above ***1 in 1,000*** for workers or ***1 in 10,000 per annum for the public*** then that risk is considered Unacceptable. These values are “evidence based” (see Section 4.7.2) and are representative of worker risk levels that may be observed in certain industries and of risks faced by the general public. It should be noted that risks which approach these levels will require significant effort to demonstrate ALARP. This is in stark contrast to “technology driving” goals, where there is much less reliance on ALARP/ALARA to drive down risk, as also described at Section 4.7.2. The HSE specifies that an annual risk of death less than ***1 in one million*** may be classed as broadly acceptable. In setting this boundary, the HSE note that this level of risk is extremely low when compared with the background level of risk that the public in general choose to be exposed to (the background level of risk is estimated at an annual risk of death of 1 in 100). Between these extremes lies the Tolerable region. Risks which fall into this category are assessed on an As Low As Reasonably Practicable (ALARP) basis. In providing advice on the meaning of ALARP, the HSE refer to case law which states: *“a computation must be made in which the quantum of risk is placed on one scale and the sacrifice, whether in money, time or trouble, involved in the measures necessary to avert the risk is placed in the other; and that, if it be shown that there is a gross disproportion between them, the risk being insignificant in relation to the sacrifice, the person upon whom the duty is laid discharges the burden of proving that compliance was not reasonably practicable.* To discharge this responsibility, the HSE provides further guidance on the use of cost-benefit analysis as a means of determining gross disproportion.
Scheme maturity:	The HSW Act was enacted in 1974. The TOR scheme was defined in 1987 and was last updated in 2001.

Table 25 Summary of Application of RAC in the GB Rail Industry

<table>
<tr><td><b>Scheme Owner / Name:</b></td><td><b><i>The HSW Act / The Railways and Other Guided Transport Systems (Safety) Regulations 2006 [17]</i></b></td></tr>
<tr><td><b>Are RAC Used?</b></td><td><b><i>Yes</i></b></td></tr>
<tr><td><b>If RAC Used:</b></td><td><b><i>Type:</i></b> The UK Rail Industry has introduced <b><i>high level individual RAC</i></b>:
• Passenger safety metric - 1.070 Fatalities and Weighted Injuries (FWI) per billion passenger kilometres
• Workforce safety metric - 0.134 FWI per million worker hours
There are no societal risk targets in existence.
The use of FWI measures was introduced because non-fatal accidents are more common than fatal accidents, and the railway wanted to find a means to capture and prioritise these accidents where appropriate. Substantial research has been completed to find the appropriate weighting, and to derive the appropriate valuation of the cost of an avoided (equivalent) fatality.</td></tr>
<tr><td></td><td><b><i>Form:</i></b> Injuries are included in the RAC, on the basis that one FWI = one fatality = 10 major injuries = 200 reportable minor injuries or class 1 shock/traumas = 1,000 non reportable minor injuries or class 2 shock/traumas.
For societal risks, although targets for UK rail operations are not specified, an <b><i>F-N curve</i></b> is plotted for hazards that could lead to multi-fatality events.</td></tr>
<tr><td><b>Brief Description:</b></td><td>The <b><i>Safety Risk Model</i></b> (SRM) is a detailed quantitative model representing 120 hazardous events and their precursors. The SRM enables the contribution to risk from lower level failures to be established. The SRM is available for use by UK rail undertakings and templates have been developed to aid the use of the SRM by external parties.
Additionally guidance is provided on how to perform a risk assessment. This guidance is complementary to the SRM. It provides:
• A simple apportionment method that enables global targets to be translated onto a risk matrix.
• Examples of how risk matrix boundaries should be scaled based on the size of the operation (e.g. the quantity of passenger journeys annually).
<table>
<tr><td colspan="3" rowspan="2"></td><td colspan="5"><b>Consequence (fatalities / event)</b></td></tr>
<tr><td>0.005</td><td>0.025</td><td>0.125</td><td>0.625</td><td>3.125</td></tr>
<tr><td colspan="3"><b>Frequency</b></td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td>1 in 12 days</td><td>31.25 / year</td><td>5</td><td>🟨</td><td>🟨</td><td>🟥</td><td>🟥</td><td>🟥</td></tr>
<tr><td>1 in 2 months</td><td>6.25 / year</td><td>4</td><td>🟨</td><td>🟨</td><td>🟨</td><td>🟥</td><td>🟥</td></tr>
<tr><td>1 in 9 months</td><td>1.25 / year</td><td>3</td><td>🟩</td><td>🟨</td><td>🟨</td><td>🟨</td><td>🟥</td></tr>
<tr><td>1 in 4 years</td><td>0.25 / year</td><td>2</td><td>🟩</td><td>🟩</td><td>🟨</td><td>🟨</td><td>🟨</td></tr>
<tr><td>1 in 20 years</td><td>0.05 / year</td><td>1</td><td>🟩</td><td>🟩</td><td>🟩</td><td>🟨</td><td>🟨</td></tr>
</table>
In these systems operational errors are integral to the risk assessment processes; that is they are modelled within the SRM in a similar manner as technical system failures. There are no specific conditions specified for operational tasks that are deemed to guarantee acceptable performance. There is however substantial research into the causes of operator errors including the identification of barriers that could minimise them.</td></tr>
</table>

Table 26 Summary of Application of RAC in the UK Offshore Sector

Scheme Owner / Name:	***UK Government Health and Safety Executive (HSE) / HSE Offshore Risk Assessment Guidance***
Scheme Coverage:	***UK Continental Shelf (UKCS)***
Are RAC Used?	***Yes***
If RAC Used:	***Type:*** High level individual risk targets A maximum tolerable individual risk of death criteria is specified as ***10^{-3} per year*** however ALARP criteria and SFAIRP criteria are additionally discussed. Group risk is considered by the majority of operators, but this is done on a voluntary basis. There is no requirement in the UK legislation to provide it.
	Form: A maximum tolerable individual risk of death criteria is specified as ***10^{-3} per year*** however ALARP criteria and SFAIRP criteria are additionally discussed. Group risk is also considered, although this is discussed in the context of integrity of temporary refuge onboard offshore installations.
Brief Description:	The HSE requires a "safety case" compliance demonstration of all relevant Statutory Provisions which includes the Health and Safety at Work Act and a number of specific offshore regulations. There is a requirement to carry out a risk assessment however this assessment can be qualitative, semi-qualitative or quantitative depending on the complexity of the installation and the magnitude of risk.  Hazard identification Risk estimation and ranking of risks Risk evaluation and Implementation of risk reduction to ensure regulatory compliance Review Identification of possible additional risk reduction In terms of specific criteria, quantitatively the ***10^{-3} per year target*** is specified on an individual basis. Until 2005 the UK HSE specified an upper frequency for Temporary Refuge (TR) impairment of 10^{-3} per annum. Since the introduction of the 2005 Safety Case Regulations this requirement has been removed. However many operators retain the demonstration that the TR impairment frequency is less than 10^{-3} as part of their demonstration that risks are ALARP. Beyond these quantitative criteria, ALARP considerations apply.
Scheme maturity:	The Health and Safety at Work Act has been in force since 1974, however it is primarily the Offshore Installations (Prevention of Fire and Explosions, and Emergency Response) Regulations 1995 and the Offshore Installation and Safety Case Regulations 2005 that provide the framework for ensuring risks are demonstrably ALARP.

Comment:	References: HSE Information Sheet: Guidance on Risk Assessment for Offshore Installations (3/2006). The Offshore Installations (Safety Case) Regulations 2005, 2005 No. 3117

Table 27 Summary of Application of RAC in the Netherlands

Scheme Owner / Name:	***Dutch Ministry of Transport, Public Works and Waste Water Management and the Dutch Ministry for Housing, Spatial Planning and the Environment.***
Scheme Coverage:	***The Netherlands***
Are RAC Used?	***Yes***
If RAC Used:	***Type:*** The Netherlands specifies high level individual targets***.*** For societal risks, F-N curves are used. The targets have evolved over time but have their foundations in the original 1953 value discussed above.
	Form: Risks are specified in terms of possibility of death per annum, as follows: • Maximum tolerable individual risk of death for new establishments: ***10^{-6} per annum*** • Maximum tolerable individual risk of death for existing establishments: ***10^{-5} per annum***, changing to ***10^{-6} per annum*** from January 2010. • Maximum tolerable individual risk of death for dangerous goods transport: ***10^{-6} per annum***. There are some noteworthy differences in the calculation of individual risk between the UK and the Netherlands. Individual risk in the Netherlands is calculated on the assumption that the individual is exposed to the risk 24 hours per day, 365 days per year. In the UK the calculation allows for exposure durations or patterns and for diverse forms of protection to be taken into account[3].
Brief Description	An undertaking covered by the requirements summarised above is required to complete a risk assessment. If that risk assessment shows that the annual risk of death is above the specified targets then that risk is considered unacceptable. However, as a consequence of setting strict and challenging goals, it has been required to allow non-compliances to be granted (for example Schipol Airport). There is a distinction made between "vulnerable" objects (houses, schools, hospitals etc) and "less vulnerable" objects (shops, hotels, commercial and offices etc). The RAC make no differentiation between public and workers. In practice the only mandatory RAC are the individual risk criteria for vulnerable objects. The remainder of the RAC are advisory. The Netherlands uses the As Low As Reasonably Achievable (ALARA) principle for achieving risk reduction. The major difference between ALARA and ALARP is that the latter requires a test of "*gross disproportion*" to be made when judging whether to select a risk reducing measure. This test is not required by ALARA, thus weighting risk reduction against costs is a much finer balancing act. In practice [31] describes that in the Netherlands showing compliance with the risk criteria is commonly accepted as the end of the process on the basis that "*the courts invariably state that, should the Government want more safety, it should put stricter levels in the Law*". Thus driving down risk through application of ALARA is far less common than the equivalent situation in the UK, where ALARP is much more forcibly applied.
Scheme maturity:	The schemes described here were updated by the Dutch Ministry for Housing, Spatial Planning and the Environment in 2004 and by the Dutch Ministry of Transport, Public Works and Water Management in 1996.

[3] It will be important for the ERA to clearly specify the basis of any RAC they choose to specify to avoid difference in terminology or calculation methodology that exists between Member States.

Comment:	The RAC in the Netherlands are an example of “technology driving” goals, which are somewhat different to the “experience based” goals used within the UK. Experience based goals are set by studying historical decisions about major hazards, particularly those that involve public discussion or scrutiny and basing RAC on this experience. Technology driving goals involve establishing RAC that represent aggressive aspirational goals, regardless of whether experience indicates that such goals are currently attainable.

Table 28 Summary of two-limit (i.e. upper limit, lower limit with ALARP/ALARA region in between) systems within EU Members States[4]

	Entities / Application	Comments
Upper limit values, fatalities per year		
1 x 10^{-3}	UK HSE	For workers
1 x 10^{-4}	UK HSE	For public
1 x 10^{-5}	Hungary	No distinction between public and workers
Lower limit values, fatalities per year		
1 x 10^{-6}	UK HSE	For public and workers
	Hungary	No distinction between public and workers

Table 29 Summary of single limit (i.e. upper limit only) systems within EU Members States

	Entities / Application	Comments
Upper limit values, fatalities per year		
1 x 10^{-5}	Netherlands	Applies to vulnerable objects in existing situations.
	Czech Republic	Limit for existing installations.
1 x 10^{-6}	Netherlands	Applies to new permits for fixed installations, new land use plans and transport of dangerous goods, including by pipeline.
	Czech Republic	Limit for new installations.

[4] The French approach to major hazards risk has traditionally been deterministic; in other words consequence based. However, recent developments in relation to Land Use Planning have introduced the general concepts of risk assessment in the form of a "***technological risks prevention plan***". The basis of this is a semi-quantitative risk based decision matrix. This decision matrix uses consequence and frequency scales as a means of arriving at a decision whether to permit a request for a new facility or a modification to an existing facility to be granted, and whether this decision is conditional on additional risk reduction measures being employed.

Table 30 Summary of Application of RAC in a Company Scheme

Scheme Owner / Name:	***Confidential***
Scheme Coverage:	***All sites internationally***
Are RAC Used?	***Yes***
If RAC Used:	***Type:*** A major international company has developed their own set of ***Company (high level) risk targets*** which represent their aspirations for safety (and environmental) performance. They are applied internationally to all qualifying sites and operate ***in addition*** to any National schemes.
	Form: The scheme is based on societal risk (F-N curve) criteria, with safety risk acceptance criteria set at different levels for: • Each facility, based on its location and the consequences of an accident (i.e. whether the consequences extend beyond the facility) • The size of each facility • Other associated activities, such as transport operations The scheme is fatality based (no injuries are included) for safety issues. In addition, non-safety consequences are also defined within the framework.
Brief Description:	In this methodology, guidance is provided on choosing the hazards that should be assessed. The methodology includes a scaling process so that facilities of differing size can be assessed and compared. However, other than this scaling process, no further lower level apportionment of the Company high level risk target has been made. To ensure a common approach standard tools and pre-defined data are supplied (these data sets are based on historical performance and include all causes of failure: technical and/or operational). Once completed, the risk assessment is used to determine the level of reporting and responsibility for action. If the level of risk is calculated to exceed an upper threshold then that must be reported to the senior management group together with proposed risk reduction measures. Example risk mitigation measures are provided. Operational tasks are not given special attention, and must be considered in the same manner as technical issues.
Scheme maturity:	Not applicable

Table 31 Summary of Application of RAC in Norwegian Rail

Scheme Owner / Name:	Norwegian National Railway Administration (NRA; Jernbaneverket)
Scheme Coverage:	***Infrastructure owner and operator. (As above) Jernbaneverket holds total responsibility for safety on their network.*** ***The RAC are used to support NRA's internal decisions, and for use to document safety to the Regulatory Body (Norwegian Railway Inspectorate).***
Are RAC Used?	***Yes***
If RAC Used:	***Type:*** There is a national requirement for railway enterprises to have qualitative or quantitative safety targets and risk acceptance criteria. Jernbaneverket has specified RAC for the following groups: • For society at large as result of activity on the Norwegian Network • Criteria for individual risk
	Form: These are specified in terms of fatality
Brief Description:	An integral part of the Safety Management System is that all changes in the system are subject to a risk analysis. The following is to be demonstrated: • Total risk level shall not exceed 11 fatalities per year. This number is based on average historical risk levels from 1980-2000. • Annual individual risk of fatality shall not exceed 1*10^{-4} for any traveller. This value is representative of the minimum annual fatality risk of young people from natural causes. It was chosen without modification for use in the railway context. • Annual individual risk for railway workers shall not exceed a Fatal Accident Risk of 12.5 per million hours worked (i.e. 1.25*10^{-5}). • The requirement to conduct ALARP assessments is an integral part of the system. The ALARP criteria is supported by a cost benefit principle based on a "willingness to pay" value of statistical lives of 25 million Norwegian Krona. For example, and using a simplified calculation, a risk reduction measure which has a cost of 2 million GBP and a life span of 20 years, is cost effective if it reduces collective risk (PLL) by more than 0.05; that is it saves one life or more over that period. Benefits in terms of avoided loss of assets or avoided environmental damage may also be included in the cost benefit evaluations. It is mandatory for improvements that meet this criterion to be implemented.
Scheme maturity:	The current scheme has been in operation since 2007, but builds on similar schemes developed initially in 2001.
Comments	The RAC determine the risk reduction strategy when planning for and implementing changes ranging from the introduction of new lines to organisational or procedural changes. In addition the NRA have short and long term goals for overall safety performance on the network which act as a catalyst the safety work in Jernbaneverket at large.

DNV

is a different kind of consulting firm, offering advanced cross-disciplinary competence within management and technology. Our consulting approach reflects the new risk agenda for both private and public sector organisations. We have a firm base in DNV's strong technological competencies, international experience and unique independence as a foundation. Our consultants serve international clients from locations in Norway, UK, Germany and Benelux.

DNV
Veritasveien 1
N-1322 Hovik
Norway
Phone: +47 67 57 99 00

DNV
Businesspark
Essen - Nord
Schnieringshof 14
45329 Essen
Germany
Phone: +49 201 7296 412

DNV
Duboisstraat 39 – Bus 1
B-2060 Antwerp
Belgium
Phone: +32 (0) 3 206 65 40

DNV
Palace House
3 Cathedral Street
London SE1 9DE
United Kingdom
Phone: +44 20 7357 6080

DNV
Highbank House
Exchange Street
Stockport
Cheshire SK3 0ET
United Kingdom
Phone: +44 161 477 3818

DNV
Cromarty House
67-72 Regent Quay
Aberdeen AB11 5AR
United Kingdom
Phone: +44 1224 335000

a different approach for a new reality:

MANAGING RISK