EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

SAFETY REGULATION COMMISSION DOCUMENT
(SRC DOC)

SRC DOCUMENT 46

Annex A
Safety Fundamentals for Safety Scanning

Edition	**:**	**1.0**
Edition Date	**:**	**14 June 2011**
Status	**:**	**Released Issue**
Distribution	**:**	**General Public**
Category	**:**	**SRC Document**

F.2 DOCUMENT CHARACTERISTICS

TITLE		
SRC Document 46 – Annex A – Safety Fundamentals for Safety scanning		
Document Identifier	**Reference**	SRC Doc 46 – Annex A
srcdoc46_annex_a_e1.0_ri	**Edition Number**	1.0
	Edition Date	14.06.2011

Abstract

This document contains the detailed description of Safety Fundamentals and basic safety regulatory principles. These Safety Fundamentals are the result of work conducted by a representative group of aviation safety and safety regulatory experts during the SESAR definition phase (i.e. Work Package 1.6). They formed the basis for the SESAR Safety Screening Tool. These Safety Fundamentals and basic safety regulatory principles were further refined after the SESAR definition phase and now provide the base line for the Safety Scanning Tool for safety regulatory purposes. These Safety Fundamentals and basic safety regulatory principles provide in essence Essential Requirements for safety risk management in aviation specifically from an ATM and Total System perspective.

Keywords		
Safety scanning	Safety Fundamentals	Safety Regulation

Contact Person(s)	**Tel**	**Unit**
Gary MORTON	+32 2 729 30 40	DSS/OVS/SAF

DOCUMENT INFORMATION					
Status		**Distribution**		**Category**	
Working Draft	☐	General Public	☑	Safety Regulatory Requirement	☐
Draft Issue	☐	Restricted EUROCONTROL	☐	Requirement Application Document	☐
Proposed Issue	☐	Restricted ESIMS	☐	ESARR Advisory Material	☐
Released Issue	☑	Restricted SRC	☐	SRC Document	☑
		Restricted SRCCG	☐	DSS/OVS Document	☐
		Restricted DSS/OVS	☐	Comment / Response Document	☐

COPIES OF SRC DELIVERABLES CAN BE OBTAINED FROM	
Oversight Division (DSS/OVS) EUROCONTROL Rue de la Fusée, 96 B-1130 Bruxelles	Tel: +32 2 729 51 38 Fax: +32 2 729 47 87 E-mail: sru@eurocontrol.int Website: www.eurocontrol.int/src

F.3 DOCUMENT APPROVAL

The following table identifies all management authorities who have approved this document.

Authority	Name and Signature	Date
Quality Control (DSS/OVS)	*« signed by Daniel Hartin »* (Daniel HARTIN)	14.06.2011
Head of Division (DSS/OVS)	*« signed by Juan Vazquez-Sanz »* (Juan VÁZQUEZ-SANZ)	14.06.2011
Chairman SCAN TF (SRCCG)	*« signed by Jos Nollet »* (Jos NOLLET)	14.06.2011
Chairman, SRC Co-ordination Group (SRCCG)	*« signed by Franz Nirschl »* (Franz NIRSCHL)	14.06.2011
Chairman, Safety Regulation Commission (SRC)	*« signed by Harry Daly »* (Harry DALY)	14.06.2011

(Space Left Intentionally Blank)

F.4 AMENDMENT RECORD

The following table records the complete history of this document.

Edition No.	Date	Reason for Change	Pages Affected
0.01	12-Jun-09	First draft.	All
0.02	02-Jul-09	Comments on first draft.	All
0.03	03-Aug-09	Final comments included, list of acronyms added and editorial changes. Document sent for formal SRCCG consultation (RFC No. 0916).	All
0.04	11-Mar-10	Update following RFC No. 0916.	All
0.05	20-Dec-10	Incorporation in Annex Book SRC-report SCAN TF.	References
0.1	01-Feb-11	Document re-numbered and incorporated as Annex A to SRC Document 46. DSS/OVS quality review. Document sent for formal SRC consultation.	All
0.2	06-Apr-11	Update following SRC consultation (RFC No. 1104).	All
1.0	14-Jun-11	Document formally released following SRC approval (RFC No. 1113).	References

(Space Left Intentionally Blank)

F.5 CONTENTS

1. INTRODUCTION

1.1 General Approach

This document provides a detailed description of Safety Fundamentals and basic safety regulatory principles, which could serve as a rationale for the use of “Safety Fundamentals” and “basic safety regulatory principles” as part of safety oversight as required by ESARR1 (2004) and/or EC 1315/2007 (2007). This oversight relates to the provision of air navigation services as for instance captured in the “Common Requirements” EC 2096/2005 (2005).

Effective safety regulatory involvement in changes to the functional ATM system (national, international such as FAB or pan-European such as SESAR) needs appropriate methodological support to provide satisfactory management of safety and safety regulatory risks related to these changes. As an example, SESAR represents a major change that comprises many inter-connected operational improvements with multi-actor involvement calling for the need to consider the dynamic interactions, as well as the new risks that will emerge from such a significant system change (cf. SESAR JU 16, 2008).

From the perspective of a competent safety oversight authority it is of great importance to gain confidence that essential needs for safety, in their widest sense, are identified in a structured and verifiable way. These identified needs are then also consequently to be satisfied in an effective and verifiable way. This confidence requires clear processes at the interface between the developers and the competent safety oversight authorities. Safety Fundamentals relate directly to safety regulatory requirements. As such, they are helpful for the initial and progressive identification of safety and safety regulatory risks resulting from changes such as national, FAB or SESAR operational concepts. The level of detail of the output of this risk identification is commensurate with the growing level of maturity of these concepts during their development. Progressive application during the development phases of a change will provide both more detailed results while allowing follow-up of earlier identified needs.

Safety Fundamentals provide a means to identify deficiencies relevant for the safety oversight and safety regulatory tasks and contribute to the oversight argument an NSA needs to provide (primarily to itself) for approval or acceptance of system changes or implementations.

1.2 Safety Fundamentals

Safety Fundamentals are not a new concept in safety science. In safety critical industries, they are recognizable as essential criteria for a safe design. For example in the nuclear industry, these criteria for a safe design are entitled “deterministic design criteria”. These deterministic rules represent firm, non-negotiable regulatory requirements. The violation of deterministic design criteria produces obvious portions of risk that require regulatory actions. They provide a resilient approach towards engineering and design.

In the nuclear industry, deterministic design describes basic safety rules, For instance a single point of failure should not lead to the breakdown of a function. Other well-known examples are the second pair of eyes (human redundancy), the fail-safe principle, or the principle of independence, which requires a clear distinction of functionalities in the system in order to avoid that failures in one part of a system affect performance of the remaining parts of the same system.

In other safety critical industries such as nuclear, these Safety Fundamentals are commonly used as a benchmark in the early licensing stages of operations (e.g. building licenses). In other words, the Safety Fundamentals enable consideration and anticipation of safety aspects, which would lead to insufficient safety performance or would eventually show up as safety critical in safety assessments.

Late identification of insufficient safety performance and/or safety critical aspects, results in business risks for the licensee such as; a denied license, additional unplanned work to meet the requirements or the total failure of a project.

In other words, Safety Fundamentals summarize safety regulatory requirements, which are essential for a licensee to achieve. They also have the potential to support management decisions when it comes to cost versus benefit considerations as they reveal the required actions to manage safety risks related to a change in the earlier stages of a project.

Air Navigation Service provision in the air transport chain is evening general more complex then other industries. Different parts of the transport chain are provided for by different stakeholders e.g. mobile communication systems encompassing line-of-sight radiotelephony, line-of-sight data link and satellite communications, or navigation systems comprising ground beacons, satellite signals and autonomous aircraft sensors. These contributions are often relevant at different times in the total process. All these contributions together however determine the safety of the total activity.

Safety Fundamentals are of a generic nature and can apply to different types of changes and concepts. As an example, the Safety Fundamental ‘redundancy’ (the presence of at least two systems with the same functionality) can be equally applied to technological design (e.g. two aircraft engines providing redundancy in the same function) as to the design of the human interactions (e.g. the human redundancy of planner/coordinator and an executive controller). In ATM/ANS “dissimilar” redundancies (e.g. radar surveillance and ADS) have to be considered as well. Safety Fundamentals refer to the safety requirements but are also of practical relevance for the licensee or for the certified aviation organisation in relation with its competent authority.

In the chemical industry, the Safety Fundamentals form basic aspects of safety oversight or auditing processes. These processes build on a review of standards throughout other safety relevant industries. Besides the experiences of the aviation industry, also the experiences from the nuclear, petrochemical, maritime and railway industries are considered in the relevant processes in the chemical industry.

2. OVERVIEW OF SAFETY FUNDAMENTALS

2.1 General Rationale Behind Safety Fundamentals

Although safety has always been the most important consideration in the aviation and ATM industry, formalized management of safety and safety oversight are relatively new. The most experienced industry seems to be the nuclear industry where these lines of thought have developed and matured over a much longer period.

The International Atomic Energy Agency (IAEA), which is the nuclear equivalent to what ICAO is in Aviation, distinguishes three major layers of safety standards:

- Safety Fundamentals: Safety Fundamentals describe basic requirements, which need to be in place at all times and at all lifecycle stages, presenting the objectives, concepts and principles of protection and safety and providing the basis for the safety requirements. In other words, these are “hard” requirements with no flexibility.
  - Safety Requirements: Safety Requirements are high-level requirements in order to meet Safety Fundamentals. They are establishing the requirements that must be met to ensure the protection of people and the environment, both now and in the future. The requirements, usually expressed as ‘shall’ statements in safety regulatory documents, find their basis in the objectives, concepts and principles of the Safety Fundamentals. If these requirements are not effectively met then measures must be taken to reach or restore the required level of safety. In other words, the Safety Requirements are “softer” and allow a certain degree of flexibility in their implementation. The Safety Requirements use regulatory language to enable them for transposition into national laws and regulations. In the legislative context of the European Union, said requirements often go directly into Community law as implementing rules, so avoiding multiple transpositions at national level.
  - Safety Guides: Guides are detailed guidance on how to meet requirements (like specific safety assessment methodologies). They provide recommendations and guidance on how to comply with the Safety Requirements. Recommendations in the Safety Guides are expressed as ‘should’ statements. It is recommended to take the measures stated or equivalent alternative measures. The Safety Guides present international good practices and increasingly they reflect best practices to help users striving to achieve high levels of safety. Each publication of Safety Requirements is under normal conditions supplemented by a number of Safety Guides. These Safety Guides can be used for developing national regulatory guides.

Identical layers of safety standards found in the basic regulatory concepts as e.g. presented by EASA (Probst, 2007). Here basic regulation is distinguished as;

- Safety objectives; safety objectives are the essential requirements (mitigation of unacceptable risks) which in the EU context can be adopted by the EU legislator or at a national level by the national legislator [in nuclear terminology unacceptable risks would lead to deterministic criteria as laid down in the Safety Fundamentals]
- Processes and specifications; Processes for assessing compliance (certification) [in nuclear terminology these would be the safety requirements], mainly identifying legal responsibilities and privileges of various legal or physical persons as well as technical specifications for hardware and software. These can be captured as follows:
  - Implementing rules: Implementing Rules clarify the obligations of the regulated persons and of the competent authorities (EASA and national administrations) in provisions with force of law (“hard” rules) and limited flexibility;
  - Certification specifications: detailed technical provisions for products, which allow equivalent or alternative measures: i.e. “soft rules” with inherent flexibility;

- Acceptable Means of Compliance [in nuclear terminology this would be the safety guides] in order to establish processes compliant with the implementing rules. Like the specifications, these are “soft” rules.

The Safety Fundamentals as described in this document directly relate to the layer of the Safety objectives / Safety Fundamentals as defined by the IAEA. Possibly, they should be considered for inclusion in e.g. the EASA system or the SES legislation. These Safety Principles describe basic or even essential requirements, which need to be in place at all times and at all lifecycle stages.

Requirements on this general level are driven by “safety-science” rather than specific industry characteristics. In other words the safety processes are established by rules independent from technology. Therefore, they can be transferred into - and need to be assumed as valid for - ATM safety as well. Whether these requirements will become part of the EU safety legislative context is yet to be decided. It will mainly depend on the further development of the SES legislation and the emerging role of EASA.

2.2 The Link of Regulatory Requirements to Safety Fundamentals

The list of references to regulatory requirements as listed in §5.2 was initially used as the basis to define the Safety Fundamentals for ATM.

The Safety Fundamentals as described in the following section are derived from applicable safety regulations from different safety relevant industries as well as from a variety of international and national safety standards. Therefore, the Safety Fundamentals might complement safety requirements not explicitly mentioned in relevant ATM regulations by including requirements from safety-peer industries. Figure 1 represents the major references used (see section 5 for details).

Figure 1: Key safety regulations used to derive the Safety Fundamentals

The distinction into the three layers and the fact of seeing regulations in a hierarchical organisation of legislation, regulation and standards is a typical representation in safety regulation (see DGTREN, 2007). It is a given that Article 1 of the Chicago Convention obliges the States to establish law. In the EU this is done at Community level for the field of aviation safety. States can supplement this law through the introduction of national legislation.

The Safety Fundamentals provide a compilation of these regulations by performing a clustering of the various existing safety regulations. Important observations that provide the basis for the clustering are independent from the industry where the requirement was originally established. These underlying observations are explained in more detail in the following sections.

2.3 Structure of the Safety Fundamentals

The widest possible spread of knowledge should be consulted in order to have the best possible result from addressing the Safety Fundamentals. This knowledge should come from people working in different areas of the affected operations (operational or technical), safety managerial experts and safety regulatory experts based on a well-accepted safety culture. Four main perspectives on safety are distinguished in a stable manner through four major aspects (Figure 2):

- (1) Safety performance – this primarily addresses the safety of the total system constituted by its parts like equipment (on the ground, in space and airborne), software, procedures and/or humans. Safety arguments should reflect this overall safety performance. Safety performance is determining the design of the functions of a system. Furthermore, safety is determined by individual safety functions (e.g. TCAS) as well as by the interaction of several sub-systems for the overall safety performance.
- (2) Operational safety aspects – this addresses the joint performance of static and dynamic aspects that people within the technological design have to work in, including the procedures (e.g. ATC procedures) they are expected to follow and the human-machine interaction with the technical systems.
- (3) Management of the performance – this addresses the role of the organisation and the way it manages the achievement of safety. This includes the specification and maintenance, and the management of safety-related human factors issues.
- (4) Basic principles of safety regulation – this addresses the legal requirements as well as specific regulatory and organizational needs.

These layers are explicit in any safety regulatory approach and are equally applicable to ATM. As an example, the basic regulatory concepts of EASA are in accordance with these layers (cf. Probst, 2007);

- Product safety - The design of each aeronautical product must be approved. This holds for changes and repairs. Each individual product must be accompanied by a certificate attesting compliance with the approved design. This is equivalent to the safety performance view. The EU legislator has already agreed a similar principle for safety critical ATM/ANS systems (e.g. Galileo) and constituents and for safety critical aerodrome equipment.
- Organizational safety - Any organization providing a safety sensitive service to the public on a commercial basis (design, manufacture, maintenance, training, air transport, aerial work, aerodrome operations, ANS...) must be certificated. Certification requires a (safety) management system. Certification can give self-certification privileges (e.g. to approve minor changes or to sign declarations). This is equivalent to the management of the safety performance view.

- Personnel safety - Any person engaged in safety related tasks (flying, release to service, training, cabin safety, rescue and fire fighting, ATC, airspace design) must comply with training and proficiency requirements, including in some cases medical requirements. Compliance with such requirements has, in the case of regulated professions, to be attested by the issuing of a certificate/license. License can give certification privileges. This is equivalent to the operational safety performance view.

The EASA concept also explicitly mentions the fourth perspective in the context of the issue of product safety, which leads to an additional category of Safety Fundamentals. This perspective relates to the issue of liabilities and responsibilities for safety, which are key issues of concern for safety regulation.

These key issues of concern are included in the Safety Fundamentals as basic principles of safety regulation. The product liability directive (Council Directive 85/374/EEC) is the common denominator for these requirements. The directive states:

- The producer shall be liable for damage caused by a defect in his product. (Article 1),
- For the purpose of this Directive 'product' means all movables … [exclusion of agriculture] …'Product' includes electricity. (Article 2),
- 'Producer' means the manufacturer of a finished product, the producer of any raw material or the manufacturer of a component part and any person who, by putting his name, trademark or other distinguishing feature on the product presents himself as its producer. … [and] … any person who imports into the Community a product for sale, hire, leasing or any form of distribution in the course of his business (Article 3),
- The producer shall be liable for damage caused by a defect in his product. Producers include manufacturers, component part suppliers, importers and anyone using a trade name or trademark. A product is defective when it "does not provide the safety which a person is entitled to expect", considering all circumstances, including the:
  - presentation of the product;
  - product's reasonably expected uses; and,
  - time the product was put into circulation.

It is to be understood that ATM related products are subject to this directive.

The Framework for the Safety Fundamentals combines these key aspects of safety and safety regulation into three different perspectives on safety (Figure 2). Each of the perspectives contains a specific list of Safety Fundamentals drawn from the existing legal and/or regulatory requirements:

- 1. Safety Performance
  - Safety Architecture and Technology
  - Operational Safety
- 2. Safety Management (including its Institutional aspects)
- 3. Safety Regulatory Principles
  - Basic principles of Safety Regulation

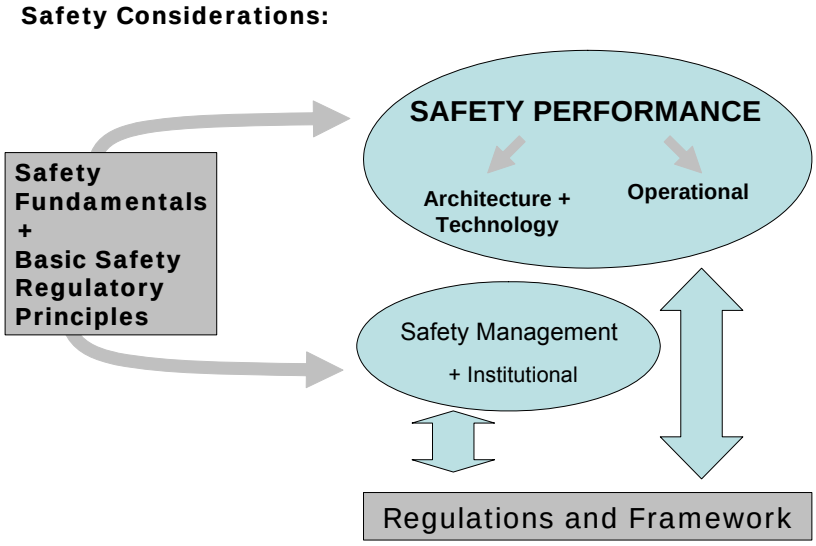

Figure 2: Safety Perspective of the Safety Fundamentals

These safety perspectives contain the relevant areas of interest that are to be addressed in a satisfactory manner to ensure that an ATM system change is as safe as possible.

One aspect to highlight is that this distinction clearly takes into account that safety is not only a system architectural issue but also a total system performance issue, which may have an impact on the safety needs of first, second or third parties.

The next section provides a rationale of the Safety Fundamentals as they are placed within these safety perspectives. For each Safety Fundamental, the following aspects will be addresses:

- The definition of the Safety Fundamental
- The detailed rationale behind the Safety Fundamental
- The manifestations for the lack of a Safety Fundamental in safety (including examples of accidents happened because of lack of the Safety Fundamental)
- Regulatory requirements stating the Safety Fundamental as a requirement

Safety Fundamentals take a “cybernetic view” on the regulatory requirements. This means, they provide a generic performance model, and allocate where the various requirements are to be found (or not to be found which would identify the need for requirements). Taking this generic view, Safety Fundamentals are generically useable for any type of system independently from the specific characteristics of the constituents in question (hardware, software, and life-ware). This cybernetic nature also allows for using the fundamentals for multi actor environments as well as a total system safety view on the entire aviation chain.

2.4 Issues the Safety Fundamentals Can Be Addressed To

Safety Fundamentals can be used to evaluate the status of a system with respect to the existing safety regulatory requirements. This applies to any stage of the systems’ life cycle, as compliance with regulation is required at all times. Specific value for the Safety Fundamentals is found in the safety regulatory impact assessments of changes or in transitions of stages of the life cycle. As Safety Fundamentals are of relevance for competent safety authorities they are at least equally important to those providers that have to answer to these authorities.

The functional ATM system, as part of the total aviation system, is a complex socio-technical system. By design, it requires the continuous collaboration of multiple actors with different roles and responsibilities (which also may change during the ATM process). Considering this, two Safety Fundamentals are of particular relevance for the ATM system. These are interdependencies as well as the need for openness and freedom of bias.

2.4.1 Safety Issues with Interdependencies

In the nuclear industry, there is a general view that about 80% of the risk contribution stems from interdependencies. Consequently, it could be concluded that risk assessment methods, which do not effectively address interdependencies have a chance of miss assessing risks by 80%.

Having a clear picture of interdependencies in a system is a key prerequisite to identify risk assessment methods that address aspects of the total system. Meeting this need creates confidence for both users and responsible organizations for safe functioning. In addition, when there are many dependencies of a different nature (e.g. human, procedures or systems) then risk assessment becomes increasingly difficult, as it may not be possible to identify these differences in terms of consistent criteria.

When understanding and accepting the importance of interdependencies a couple of underlying issues related to interdependencies can be addressed. Examples are; the risk of not sufficiently identifying interdependencies due to lack of understanding or description of the overall system, lacking redundancies in the overall system or missing good understanding of the functionality and integrity of the processes.

Most concisely, Perrow (1999) described the need to look into interdependencies with increased integration and automation. Perrow expressed the need for independence using the distinction between high cohesion and low coupling. This distinction raises the requirement for well-defined roles and responsibilities (interfaces) in a well-defined time-frame (high cohesion) and the absence of error propagation through the interfaces (low coupling).

Because ATM is a “human-centred system with a high level of automation”, a major source of interdependencies results from the human and organisational contribution to risk.

These human and organizational aspects are commonly dealt with by using Human Reliability Assessment (HRA) Methods. Independent from the technical domain, it needs to be concluded that currently available HRA methods provide only rudimentary approaches how to model interdependencies or organisational contributions within quantitative risk assessment with little regulatory acceptance (cf. OECD, 2004).

2.4.2 Safety Issues with Openness and Freedom of Biases

Tactical Safety Management requirements, applicable inside one certified organisation, emerged over the last decade in safety relevant industries. In particular worth mentioning are safety management requirements in nuclear (e.g., IAEA INSAG 13, 1999) or in ATM (ICAO SMM, 2007). Besides the general ambition for a continuous improvement of safety managerial performance using the so-called plan-do-check-act cycle, all requirements emphasize the need for improving the safety culture.

The term safety culture was coined after the Chernobyl nuclear disaster where managerial decisions influenced the behaviour on the working level in such a way that the reactor protection system was overruled by the personnel resulting in a catastrophic accident. Another example is the Challenger accident where political decisions in management led to knowingly overriding important safety information on the engineering side resulting in the loss of life and discredit of the program.

Looking at these examples, safety culture could be seen as the glue, which is required to make a Safety-Management-System work. Usually it is requested to have an open and trustful communication in order to avoid running into critical safety issues and an appropriate questioning attitude of the personnel.

In regulatory requirements, usually this organizational glue is expressed in one of the following views: (1) Safety culture is the superior requirement and a Safety-Management-System needs to be designed in such a way that a safety culture will be established (e.g. IAEA, 2006). (2) The processes in a Safety-Management-System need to be designed in such a way that key aspects of safety culture, like the trustful and open communication, are enabled by the Safety-Management-System.

As an example, IAEA DS 338 (2005) states the following requirement for the Management-System for facilities and activities. They;

- Need “to improve the safety performance of the organization through the planning, control and supervision of safety related activities in normal, transient and emergency situations” and
- Need “to foster and support a strong safety culture through the development and reinforcement of good safety attitudes and behaviour in individuals and teams so as to allow them to carry out their tasks safely.”

Independent from the way safety culture and safety management are related to each other, the superior requirement is to have both, a Safety-Management-System and a true safety culture. Safety culture may be defined in this context as the assembly of characteristics and attitudes in organizations and individuals, which establish that, as an overriding priority, protection and safety issues receive the attention warranted by their significance aiming specifically at learning and questioning these attitudes at every level of the organization.

Nowadays this original concept of “tactical” safety management inside one organisation has to be complemented by additional perspectives:

- “Strategic” safety management in order to assess potential risks and mitigate the non-acceptable consequences, before a change is implemented (e.g. based on ESARR 4) and in particular by validating new concepts during their development phase (Art. 8b.5 of the second extension of the mandate of EASA, as approved by the European parliament on 25 March 2009);
- Inter-organisational safety management where multiple actors are involved in safety related (and inter-related) activities (ref. essential requirement for aerodrome operators to establish formalised interfaces with other relevant actors);
- External feedback loops to the plan-do-check-act cycle inside one organisation, such as:
  - Independent operational monitoring of complex systems (e.g. RVSM or EGNOS in relation to GPS);
  - Safety data collection and analysis by authorities at national and EU level as per Directive 2003/42;

- Traceability of actions (or replies) following safety recommendations issued by independent Accident Investigation Bodies, as established by Directive 1994/56.

2.5 Issues with the Scope of a Safety Statement

Setting the context is most essential for an appropriate safety statement, either on safety performance of a system, the appropriateness of a safety assessment or the appropriateness of an oversight activity. Guiding questions related to scoping are:

- What is the level of maturity of the Subject?
- Who is affected by the Subject and why?
- Has the goal of the Subject been jointly set by the stakeholders?
- How much would the implementation of the Subject change the functionality and the boundaries of the current situation?
- Are there any constraints for implementation of the Subject?

3. RATIONALE FOR SAFETY FUNDAMENTALS

3.1 Safety Fundamentals for Safety Regulation – Basic Principles of Safety Regulation

3.1.1 Regulatory Principles for Independent Oversight

The definition of the Safety Fundamental

Independent Oversight comprises that the standards of safety to be achieved should be approved and monitored (i.e. oversight) by a competent body acting in the public interest, which is independent of service providers and designers/producers.

The detailed rationale behind the Safety Fundamental

The standards of safety to be achieved should be authorized and monitored (i.e. oversight) by competent body acting in the public interest, which is independent of service providers and designers/producers. In the current ATM environment, these competent bodies (that have a legal basis) are present at three levels i.e. Global (ICAO), European (EC/EASA) and National (Ministries of Transport, CAAs and/or NSAs). These competent bodies have their own oversight activities i.e. USOAP (ICAO), EASA standardisation inspections and national oversight activities

The manifestations for the lack of a Safety Fundamental in safety

Safety oversight should be organizationally separate from those responsible for designing, planning, producing, implementing and operating services or products. For European ATM this requirement is captured in EC 1315/2007 (EC, 2007). Organizational separation implies a transparent set up of communication structures in order to prevent developing gaps.

The requirement for independent verification is an essential feature in any Safety-Management-System. The second pair of eyes is essential for all safety relevant work. Many service providers are performing benchmarking in order to ensure working according to the best standards. Benchmarking is also increasingly performed between industrial domains in order to learn from the experiences in other industries (VDI 4006). The competent oversight authority forms the “outer loop” of such an independent check in some kind of “overarching cycle for the management of safety” (Leveson, 2002).

The Safety Fundamental as a regulatory requirement

The requirements for independent oversight are part of any regulation on safety management (ICAO, 2007, IAEA, 2006).

Usually also competent oversight authorities are audited against regulatory standards and perform international benchmarking with other oversight bodies.

3.1.2 Structural Needs – Legal Mandate & Ability for Ensuring a Safe Standard

The definition of the Safety Fundamental

Ensuring a Safe Standard comprises the duty of all service providers and designers/producers to take all reasonable precautions to ensure that their services or products are safe.

Guiding questions are: Is an organization considered to work according to the state of the art? Is an organization eager to update its safety standards according to recent developments of the standards? Is an organization benchmarking its results with other organizations? How is the competence of an organisation attested (e.g. certification by aviation authority; self-declaration; quality system certified by a third party)?

The detailed rationale behind the Safety Fundamental

All service providers and designers/producers have a duty of care to take all reasonable precautions to ensure that their services or products are safe. This duty of care is de facto subject to national legislation and national and European regulation and service providers and designers/producers may be held accountable for the execution of their duties as this rationale is based on societal interest in safety.

This involves having a sound, logically inferable, and traceable approach to safety, which also addresses permanent improvement of safety as required in any Safety-Management-System.

The manifestations for the lack of a Safety Fundamental in safety

ICAO requires the establishment of a State Safety Program to meet this safety fundamental. It is stated:

- In establishing States' requirements for the management of safety, ICAO differentiates between safety programmes and Safety-Management-Systems (SMS) as follows;
  - A safety program is an integrated set of regulations and activities aimed at improving safety,
  - A Safety-Management-System (SMS) is an organized approach to managing safety, including the necessary organizational structures, accountabilities, policies and procedures.

Herewith the approach of ICAO, which follows the principle of "separation" between States' and operational responsibilities adopted by the ECAC Ministers in 1997 and subsequently enforced by the SES legislation, is wider than just implementing a Safety-Management-System inside organisations. Of course it has also a wider view in order to improve the overall safety framework continuously. A State safety program will be broad in scope, including many safety activities aimed at fulfilling the programme's objectives. A State safety program embraces those regulations and directives for the conduct of safe operations from the perspective of aircraft operators and those providing air traffic services (ATS), aerodromes and aircraft maintenance.

The State safety programme may include provisions for such diverse activities as incident reporting, safety investigations, safety audits and safety promotion. To implement such safety activities in an integrated manner requires a coherent SMS. It is expected that within the EU context, the concept of a State Safety Program will be implemented as an European Aviation Safety Program with a clear and systematic distribution of responsibilities at a central and national level, based on EU legislation.

The Safety Fundamental as a regulatory requirement

The common denominator for this fundamental is product liability, which is a basic requirement for all products produced (EC, 1985).

Almost all regulations for Safety-Management-Systems require enhancing Safety-Management-System according to the state of the art on safety. This is a legally based requirement. In order to fulfil this requirement, ICAO requires a safety program aiming at enhancing the Safety-Management-Systems framework continuously (ICAO SMM, 2007).

IAEA has introduced a five-years rule for reconsidering the validity of regulations (IAEA, 2006). The “Five years rule” ensures that safety requirements are kept up to date. Five years after publication, they are reviewed to determine whether revision is necessary. Note that the “5 years rule” has its origin in the legal responsibility of a competent oversight authority to conduct safety oversight according to the state of the art. A violation of this rule could be interpreted as potential negligence of the competent oversight authorities in legal proceedings following accidents.

3.1.3 Implementation Needs for Responsibility for Safety

The definition of the Safety Fundamental

Responsibility for Safety builds on the understanding that the prime responsibility for the safety of a service or product rests with the service provider or designer/producer.

Guiding questions are; Can responsibilities be clearly allocated to parts of the institutional system? Are there any responsibilities considered as shared? Are sufficient legal documents available to demonstrate the formal sharing of responsibilities? Do the legal documents take into consideration the apportionment of liability in line with the shared responsibilities?

The detailed rationale behind the Safety Fundamental

The prime Responsibility for Safety of a service or product rests with the service provider or designer/producer. In the current ATM environment, this refers to the ANSPs and providers that have chosen to provide their services in this industry.

An appropriate interface is needed, in order to discharge the responsibility for safety, between regulated organizations and their independent safety oversight authorities. This interface needs to include a well laid-out sharing of operational experience and trustful relationship (BMU, 2009).

The manifestations for the lack of a Safety Fundamental in safety

A lack in Responsibility for Safety would immediately lead to an unknown status about the safety performance and would likely allow for a decrease of the safety status of an organization and for latent errors in the system.

In complex automated systems with technical human and organizational elements, responsibility for the overall system safety performance is split between controllers, engineers, management and manufacturer. Therefore, the need to have these actors striving together for safety is an essential feature of the current as well as the future ATM system.

Many nuclear occurrences of the last years revealed the need for having a better oversight of the responsibilities for safety of components suppliers (IAEA 2000/2001).

The Safety Fundamental as a regulatory requirement

In order to ensure a proper Responsibility for Safety it is necessary that the roles in safety management and safety regulation are sufficiently supported and communication means are clearly laid out between all parties responsible for the overall safety (ISO 9001, 2000; IAEA SG-Q, 1996; ICAO SMM, 2007).

In order to achieve this, many established regulations in the nuclear industry require explicitly that the Safety-Management-System should also enclose processes that allow a trustful and open interface between licensees and regulators as well as between licensees and suppliers (BMU, 2009).

3.1.4 Needs for New Regulations

The definition of the Safety Fundamental

Safety regulations need to be kept up to date in order to reflect the state of the art in safety. Usually (outside ATM) five years after publication, standards are reviewed to determine whether revision is necessary.

The detailed rationale behind the Safety Fundamental

The “5 years rule” has its origin in the legal responsibility of the competent safety oversight authority to oversee safety according to the state of the art. A violation of this rule would imply potential negligence of the oversight authority in legal proceedings following an accident.

Also, there is usually a public hearing of the industry when regulations are produced, amended or changed. This hearing validates the realism of the rule and ensures buy-in from the industry.

The manifestations for the lack of a Safety Fundamental in safety

Lack of the fives years rule might lead to unnecessary complexity of the regulation framework as updates need to be reflected in new regulations while the obsolete ones are still officially published. This might also lead to disproportional or cost intensive evaluation which regulation is valid.

The Safety Fundamental as a regulatory requirement

In the nuclear industry, this rule is well established (IAEA, 2005). In ATM, the five years rule is not yet established but suggested in the context of the SESAR definition phase (SESAR Consortium, 2006).

3.2 Safety Fundamentals for Safety Management

The Safety Fundamentals for Safety Management are usually expressed in the form of a ‘’plan-do-check-act”-loop. This applies to any management system in general. The methodology “Plan-Do-Check-Act” comprises to establish the objectives and processes (plan), to implement the processes (do), to monitor and measure processes and product against their requirements (check), and to take actions for continuous improvement of performance (act). An important initial step to initiate the PDCA cycle is the joint goal setting by all stakeholders involved in the air transport operation (SAFMAC, 2007).

In relation to safety, PDCA implies that; safety targets are established, safety activities need to be planned, the goals of these activities need to be both achieved and proven, and safety performance needs to be improved. Within ESARR 3 and the EC Common Requirements (EC, 2005) these steps are also referred to as; policymaking, planning, safety achievement, safety assurance and safety promotion, see figure 3.

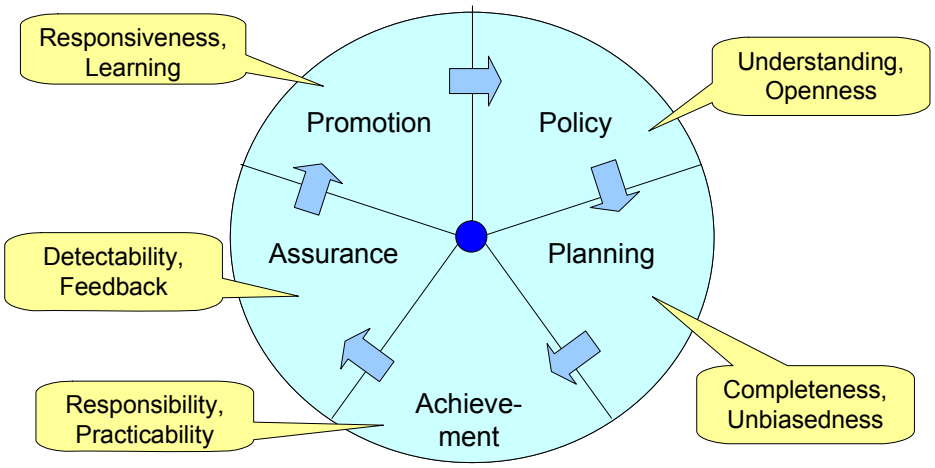

Figure 3: Safety Management perspective

3.2.1 Understanding and Openness in the Safety Policy

The definition of the Safety Fundamental

Understanding and Openness is defined as the degree to which both the commitment to safety and setting out the strategic safety aims is performed in such a way that all opinions and considerations within an organization or from other organizations are taken into account in the safety policy. Understanding and Openness are essential elements of an effective safety culture and are key requirements to an SMS and the safety oversight confidence in the operation of an SMS. They need to be established by appropriate safety education.

Guiding questions are; Is there a balanced understanding about the complexity of the problem? Are targets, objectives and issues openly discussed before they are established? Is the strategic safety management properly addressed and implemented? Is the inter-organisational perspective properly implemented? How can Small and Medium-Sized Enterprises benefit from lessons learned and best practices originated elsewhere?

The detailed rationale behind the Safety Fundamental

Openness and understanding is needed to establish a commitment to safety throughout the organisation and setting out the organisation's strategic aims while giving consideration to possible objections within an organization.

Understanding and Openness are well-established Safety Fundamentals of safety management. They deal with the fact that different persons have different experiences and knowledge that in total need to be taken into account to ensure a good safety performance carried by the total organization.

The manifestations for the lack of a Safety Fundamental in safety

Most accidents can ultimately be traced to inadequacy in the safety policy, namely not striving for openness and understanding, although the link is rarely made explicit and often difficult to prove. The importance of the Safety Fundamentals for safety can be demonstrated based on the investigation of NLR, the Aviation Research Centre of the Netherlands, on the interrelation between different aviation players, like airlines, air traffic control service providers and regulators (Roelen et al., 2003);

"The work of the FAA [US Federal Aviation Authority] Certification Process Study (CPS) Team is very relevant as this team examined interfaces between certification, maintenance, and operations. Among the conclusions of the CPS team are the following:

Critical information may not be available to those that could act upon it. Organisational barriers to communication, failure to recognize the need to communicate, information overload, and language differences, may all contribute to information flow breakdowns.

Significant safety issues learned through accidents are sometimes lost with time and must be re-learned at a very high price.

Traditional relationships among the regulators and industry have inherent constraints that have, in some cases, limited the ability to effectively identify and act on accident precursors. Further safety improvements will require significant intra- and inter-organisational cultural changes to facilitate a more open exchange of information. Regulatory solutions alone cannot achieve the desired results."

The Safety Fundamental as a regulatory requirement

Openness and understanding are key requirements of safety culture (IAEA INSAG 13, 1999; ICAO-SMM, 2007). Safety management regulations do explicitly require these as part of a Safety-Management-System (BMU, 2008; DGTREN, 2007). Some regulations also state the requirement for the underlying human attitude, the so-called questioning attitude found as important for organisational influences on events.

3.2.2 Completeness and Freedom from Bias in Safety Planning

The definition of the Safety Fundamental

Completeness and Freedom from bias are defined as the appropriateness of the aims of the organization, the resources and management structure chosen and the processes established in order to come to the best safety-related solution.

Guiding questions are; Is the envisaged change transparently and clearly laid out? Are the plans complete and without biases towards certain technical or organizational solutions? Are biases considered in the targets and planning? Is the operational transition properly planned and applied?

The detailed rationale behind the Safety Fundamental

Completeness and Freedom from bias are well-established Safety Fundamentals of safety management. They address how appropriate the planning of an organization is with respect to safety. It is essential in this planning to retain a good existing safety practice and to find the most appropriate solutions from the safety point of view. In order to achieve this, one needs to have an unbiased discussion of alternatives and deficiencies in the system and methodologies in order to have as complete as possible a basis for decisions and actions.

The manifestations for the lack of a Safety Fundamental in safety

Biases are normal human mechanisms and well known psychological issues with considerable potential effects on safety because they lead to a focus on pre-conceptualized solutions without reflecting the complete picture of a situation. They are the downside of effective human decision-making. Their role in human errors is a well investigated and established knowledge in safety (Tversky & Kahneman, 1974; Reason, 1990).

Examples on the role of biases for safety are for instance biases towards certain design solutions ("What I know is the best") or biases based on past success ("We did it like this all the time"). Teamwork with different expertises may prevent the effect of individual biases.

Biases are not limited to the operational level of an organization but exist on all levels. The challenger accident is a good example of biases on the managerial level, which were in addition, reinforced by political pressure to launch the shuttle despite some safety concerns. This bias suppressed important safety information pointed out by the engineering level and eventually led to the disaster.

As demonstrated by the challenger example, biases usually come into existence if there are contradicting aims in an organization. In the case of the challenger disaster, this was the trade-off between the safety considerations regarding the sealing of the solid rocket boosters on the engineering level versus the intention to launch the shuttle for political reasons on the managerial level.

The Safety Fundamental as a regulatory requirement

From the oversight point of view, biases are essential for safety and need to be taken carefully into account (IAEA INSAG 13, 1999). There are several regulatory principles established in the Safety-Management-System requirements to compensate for biases:

- Safety-Management-Systems require independent reviews of an organization (using audits) in order to judge about the organizational performance towards safety (ESARR 1, 2004),
- Integrated safety management systems are requiring clear and transparent processes on how decisions are taken and how the safety objectives are taken into account in business planning (e.g. BMU, 2009),
- Process descriptions are required to achieve thorough thinking about the ways an organization works and to describe (and iteratively improve) the processes of decision making in order to balance different objectives (ISO 60300, 2007).

3.2.3 Responsibility and Practicability in the Planning of Safety Achievement

The definition of the Safety Fundamental

Responsibility and Practicability are defined as the detailed means of translating the plan into reality by means of clear responsibilities for and practicability in safety achievement. The fundamental Responsibility could either address responsibilities within networks or complex systems or legislative responsibilities.

Guiding questions are; is the allocation of safety responsibilities complete and in line with applicable legislation? Are responsibilities clearly and unambiguously allocated? Are there cases of unnecessary duplication of provisions? Are well working processes maintained after a change or in a new concept?

The detailed rationale behind the Safety Fundamental

For translating a plan into reality there first is a need to have a clear allocation of responsibilities within a organization as well as between organizations in order to ensure proper safety achievement. In addition, a second aspect is the requirement to have a practically feasible process to perform the work. If the planned process is not practically feasible this may lead to shortcomings or deliberate deviations of staff from the plan and hence to potential safety issues.

Responsibilities cannot be shared but only transferred. Assuming shared or absence of responsibility for safety makes it unclear how to proceed and how to decide in case safety issues occur.

Responsibility and Practicability is also an issue between organisations. In airborne separation modes, for instance, responsibility needs to be delegated from the controller to the pilot and back from pilot to controller. This increases the coordination effort required in the transition states from ground to airborne separation modes (SESAR JU 4, 2008)

The manifestations for the lack of a Safety Fundamental in safety

Without clear allocation of responsibility, no management system would work effectively and required safety functions would deteriorate because no one is dedicated to maintain and improve them according to the Plan-Do-Check-Act principle. Consequently, clear responsibilities are binding requirements for any management system (IAEA, 2006; ICAO-SMM, 2007).

ISO 9001 states that management shall develop, implement, and maintain a quality assurance program with a clear organizational structure, functional responsibilities, levels of authority and interfaces for those managing, performing and assessing the adequacy of work. The QA program is binding on all personnel, including those with responsibility for planning or scheduling resource consideration (ISO 9001, 2000).

The Safety Fundamental as a regulatory requirement

From the safety oversight perspective, clear responsibilities are required in order to have an oversight (and if so required, a legal) interface to the regulated organization. Accordingly, the management structures, responsibilities and accountabilities for safety need to be clearly defined throughout the organization and in supporting organizations (ESARR 1, 2004; INSAG 13, 1999; IAEA SG-Q, 1996).

3.2.4 Detectability and Feedback in the Planning of Safety Assurance

The definition of the Safety Fundamental

Detectability and Feedback are defined as the detectability of safety issues by continuously monitoring safety performance (feedback) in order to realize safety assurance.

Guiding questions are; Are potential problems in principle detectable (e.g., via safety indicators)? Is feedback established or can it be established (e.g., data sharing between two independent organizations)? Can systematic analysis of automatically recorded data be useful? Is an independent operational monitoring necessary? Is the information from the “external” feedback loops properly analysed and used for improvement?

The detailed rationale behind the Safety Fundamental

Some part of the system must be able to detect the failure of either itself or another part of the system. Once detected, the faulty part must make no further contribution to the behaviour of the system any more (fail-safe principle; see integrity) and also the system must be able to compensate for the lost functionality (fault tolerance; see redundancy).

Essential elements of these Safety Fundamentals are accident investigation and prevention processes, which are used to continuously monitor safety performance to ensure timely corrective action, and periodic surveys to enable improvements.

The underlying cause of the Linate runway incursion was the absence of a functioning Safety-Management-System on the airport, which indicates, among other things, a failure of assurance. In the Überlingen collision, the tolerance towards unofficial rest practices indicates a failure in detection and feedback.

The manifestations for the lack of a Safety Fundamental in safety

Lack of feedback means flying in the blind and taking risk not to improve the system based on past experiences. Hence, the need for implementing incident reporting and improvement processes is a vital key for any Safety-Management-System.

The Safety Fundamental as a regulatory requirement

Operational feedback programmes were “the early safety management systems”. They exist in many industries from their beginnings in order to investigate safety issues and to avoid severe incidents or accidents.

From the regulatory perspective, they are a key means to oversee and judge about the safety performance of the industry and are therefore laid down as key elements in any safety management regulation (ICAO-SMM, 2007; IAEA/NEA 1998; DG TREN, 2007).

3.2.5 Responsiveness and Learning in the Planning of Safety Promotion

The definition of the Safety Fundamental

Responsiveness and Learning are defined as the way of ensuring a continuous improvement process, timely corrective actions (responsiveness) and dissemination of lessons learned (learning) Promotion

Guiding questions are; Can learning processes be established? Is the system able to be modified in a timely manner? Are there aspects slowing down learning or system modification? Can authorities properly respond to urgent safety needs?

The detailed rationale behind the Safety Fundamental

Not being able to timely respond to changing demands or an incompletely defined service often leads to the fact that safety problems persist for a long time and work-around solutions are developed. This potentially, leads in the long term to violations. Especially when systems are complex with many involved stakeholders, the time needed to implement a required change might drastically increase.

The manifestations for the lack of a Safety Fundamental in safety

Any system needs to be effective in the way safety is improved. However, complex systems with lots of internal and external suppliers may be sluggish in the reaction - even on very critical safety related events. Improvements might be initiated too late. Knowledge gained by further development of the “state of the art” in system technology or procedures might be considered too late or too slow for improving the system. In both cases latent weaknesses persist, safety issues remain without improvement with the potential to lead to safety critical events.

The Safety Fundamental as a regulatory requirement

Such a situation is critical from the safety regulatory point of view. If information from an event is not used timely to improve the system, the organization could be addressed in a legal action for injunction (i.e. safety regulatory risk). If the development of "state of the art" is not well taken into account, legally the organization could possibly run into an issue of negligence (IAEA, 2006).

In order to fulfil its regulatory responsibility to act for the health and safety of the public, safety regulatory bodies need to address the lack of responsiveness.

Several levels exist in regulation to ensure oversight of responsiveness in organizations like the requirement to report the results of an incident investigation within a specific timeframe (RSK, 2008); periodic safety assessments (in the nuclear industry every 10 years) to check the overall status of a system (BFS, 2004). Standards providing underlying guidance on the methodologies used need a continuous update every five years in order to keep the required methodologies up to date and valid.

3.3 Safety Fundamentals for Safety Performance – Operational Safety Aspects

Figure 4 outlines the set of Safety Fundamentals on safety performance with respect to operational safety aspects.

Operational tasks are conducted in a so-called human-machine system. A human has a task, technical system(s) to support in performing the task and is in ATM related to other humans having their own human-machine system (MMS).

Within the MMS, humans are considered as being goal oriented (e.g. the goal of a controller is to optimize the overall performance within the sector), not purely focussed on accomplishing one specific task (e.g. dealing with one specific conflict). The task and other conditions set in the MMS should be such that the human can accomplish a task while not conflicting with the overall performance goal. Resilience comes in through the ability of a human to recognize when goal and conditions do not fit the competence.

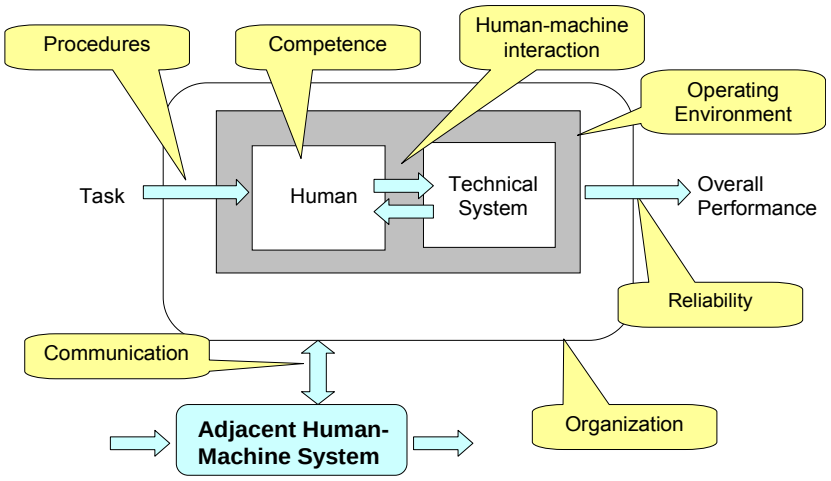

Figure 4: Operational Safety Aspects perspective

3.3.1 Procedures

The definition of the Safety Fundamental

Procedures describe what is required by the human operators to deliver a service, i.e. the processes to operational support. It includes definition of roles and responsibilities, procedure structure, content, detail, and realism. From the regulatory point of view it is necessary to clearly identify the responsibilities of different actors: e.g. the airspace designers, the inspectors for in flight calibration, the AIS providers and the providers of digital data to avionics, in relation to instrument flight procedures.

Guiding questions are; Are there vague elements in how the task looks like? Is the task already well described in written procedures?

The detailed rationale behind the Safety Fundamental

Procedures are a well-established aspect of safety. Over- and under-proceduralisation are leading to safety issues. Over-proceduralisation leads to less flexibility, which is on the other hand needed for unforeseen situations while under-proceduralisation leads to lack of consistency in the operations, which then gives opportunity for acting outside the safe operational boundaries.

The manifestations for the lack of a Safety Fundamental in safety

As an example, accidents, almost by definition, involve some form of deviation from procedures. The Überlingen collision resulted in part from an unofficial practice of the second controller resting during the night shift, which is a type of deviation from planned procedures. It also revealed that procedures on response to conflicting ACAS and controller instructions had not been standardized throughout the industry. The Los Angeles runway incursion (1st February 1991) involved controller errors that were attributed to a failure of the ATSU to implement adequate procedures.

The Safety Fundamental as a regulatory requirement

Existence of and adherence to procedures are an essential part of safety regulatory approval and ongoing oversight activities. In addition, changes implying procedural changes need to be checked against consistency within the overall procedural framework. Therefore, the aspect of procedures is an essential aspect of regulation (IAEA NS-R-2, 2000; ESARR 5, 2005; EC, 2006).

3.3.2 Competence

The definition of the Safety Fundamental

Competence is defined as the capabilities of the staff working on the technical and procedural aspects of the system. It could be competence of controllers, pilots but also engineering, maintenance and other safety related staff, management, regulators or competent safety oversight authorities.

Guiding questions are; Does the current competence fit the technical and operational aspects? Can competence be built up in time? What are the obligations of the employers in relation to non-regulated professions?

The detailed rationale behind the Safety Fundamental

The competence required to operate a system and to provide the intended service includes training needs, training methods, competence standards, trainer roles/competence, transition from classroom to on-the-job training, effects on operational task performance etc.

The manifestations for the lack of a Safety Fundamental in safety

For example, the American Airlines accident following a wake turbulence encounter (12th November 2001) was in part attributed to training methods that resulted in excessive rudder input to correct the initial roll motion.

The Safety Fundamental as a regulatory requirement

Human capabilities are an essential part of safety regulatory oversight. In any industry, regulations set competence and staffing requirements (IAEA, 2005, WENRA 2003; IAEA NS-G-2.8, 2002). Well known in Aviation are the legally required regular competence checks (e.g. flight crew licensing; ICAO Annex 1, 2009).

3.3.3 Human-Machine Interaction

The definition of the Safety Fundamental

Human-machine interaction is defined as the quality of the interaction between the system and the human resources required to operate it and to provide the intended service.

Guiding questions are; Are there ergonomic problems or improvements with the system change? Are specifications compliant to ergonomic standards? Are the procedures clear when greater safety margins (e.g. larger separations) have to be established in the shortest possible time following a system failure?

The detailed rationale behind the Safety Fundamental

The quality of the interaction between the technical system and the human resources is essential to provide the intended service. It includes in particular workplace design, workstation ergonomics, usability, working environment, and job-induced fatigue.

System and equipment complexity are performance factors influencing human reliability. Examples include: Complexity and amount of equipment; functional dependencies or dependencies between control systems, safety systems or barriers. Other factors mentioned in some regulatory materials are unclear logic in the task flow or work methods, lack of standardization of codes, poor ergonomics of controls or components, or improperly marked and difficult to recognize or understand control elements (FAA, 2009; ICAO Doc 9683).

The manifestations for the lack of a Safety Fundamental in safety

Examples with ergonomic issues are numerous in all industries. Well known in the nuclear industry is the Three Mile Island accident on 28th March 1979. In Aviation, the A320 crash at Strasbourg on 20th January 1992 is a classical example (VDI, 1992). Also the Überlingen accident (1st July 2002) was in part the result of the controller attempting to make use of two adjacent workstations, which is also a type of human-system interaction problem.

The Safety Fundamental as a regulatory requirement

According to the importance of ergonomic design for safety, numerous regulations exist in almost any industry.

3.3.4 Operating Environment

The definition of the Safety Fundamental

The Operating Environment is defined as the conditions under which the system operates such as variations of weather conditions, type and amount of traffic, airspace classification, etc.

Guiding questions are; which are the environmental conditions (like light noise, weather etc.) under which the work needs to be performed? Are there any impacts from local conditions to be considered (e.g. geographical aspects for an airport such as terrain)?

The detailed rationale behind the Safety Fundamental

Environmental aspects are important conditions for human performance, which need consideration at the design stage because they are usually not modifiable. These conditions could negatively influence human performance (IAEA NS-R-2, 2000).

As an example, airports usually need to make a trade off between the safest, most economic and environmental friendly approach path. Geographical constraints may lead to a permanent influence on pilots or controllers in such a way that not necessarily the safest trajectory on approach or departure is flown.

Another example might be that manual control capabilities of pilots (in flying conditions) might deviate from those of controllers on the ground. Hence, concepts of human-machine interaction as developed for controllers will not work for pilots in the same way if pilots should perform airborne separation.

The manifestations for the lack of a Safety Fundamental in safety

Lack of consideration of the operating environment might lead to long-term safety threats. Short runways, difficult wind conditions etc. are regular threats to aviation. The discussions on the weather conditions related to the loss of an Air France aircraft over the Atlantic ocean (1st June 2009) are a possible example.

The Safety Fundamental as a regulatory requirement

Environmental aspects usually play a major role in initial regulatory approval, e.g. Airport regulations. Also in other industries, regulations exist to address industry specific environmental influences. The so-called Seveso-directive (Council Directive 82/501/EEC on the major-accident hazards of certain industrial activities), the more general Directive 2003/105/EC of the European Parliament and of the Council of 16 December 2003 was issued to generalize the requirement to other technical domains.

More specifically related to the direct working environment is for example IAEA SG-Q (1996). It states that

- “Suitable working environments shall be provided and maintained so that work can be carried out safely and satisfactorily, without imposing unnecessary physical and psychological stress on the plant personal” and,
- “HF influences the effectiveness and fitness of personnel for duty, e.g. frequency and clarity of communication, limits of the duration of work time.” This element however also overlaps with the Safety Fundamental of human-machine interaction.

3.3.5 Organisation

The definition of the Safety Fundamental

Organization is defined as the managerial aspects of the working environment.

Guiding questions are; are resources needed to perform on the operational level sufficiently available? Is the static or dynamic structure of work processes changing? Are inter-organisational aspects to be considered? Are proper safety arrangements with, or safety oversight of sub-contractors in place?

The detailed rationale behind the Safety Fundamental

Organization is covering the managerial aspects of the working environment, which is a well-established aspect for safety. The human resources required to operate the changed ATM system and to provide the intended service are decisive for safety. They include in particular staff availability, staff selection criteria, organizational structure, shift patterns, team structures.

The manifestations for the lack of a Safety Fundamental in safety

The role of the organization is a well-recognized aspect for safety (Reason, 1997).

As an example the Überlingen accident (1st July 2002) was in part the result of inadequate staffing for night-time operations in the ATCC as well as managerial decisions.

The Safety Fundamental as a regulatory requirement

Because of their importance, organizational requirements like staffing or education of staff are usually covered in safety regulatory requirements (e.g. ICAO-SMM, 2007; IAEA DS 338, 2005).

In the last years, where the aspects of safety management are being established throughout safety critical industries, the importance of the aspects of the organization of a service is even more highlighted. Specific requirements are being established like open communication, safety culture, clear organizational requirements to deal with conflicts in organizations etc (example: IAEA INSAG 13, 1999). The OECD (2008) requires from any nuclear organization to establish a free-of-conflict environment within the organisation.

The Safety Fundamental Organization therefore partly covers requirements, which belong to the group of Safety Fundamentals on safety management as well (see section 3.2).

3.3.6 Communication

Communication is defined as the interaction between people, also including aeronautical telecommunication.

Guiding questions are; Is the system changing the way of communicating? Are important current ways of communication changing? Are there new ways of communication? How well is the communication system aligned to the tasks that need to be performed?

The detailed rationale behind the Safety Fundamental

Communication between and amongst different players in the ATM delivery like controllers, maintenance staff, manufacturers, management, oversight staff and regulation staff is key for safe operations.

The procedures for communication between controllers, flight crew, planners, engineers and ATC managers include communication procedures, communication workload, standard phraseology, language training issues, information content (e.g. callsign distinction), coordination and handover procedures, personal inter-relations as well as organizational inter-relations etc.

In addition, the mix of data-link environments and communication based air-ground communication are aspects of this Safety Fundamental.

The manifestations for the lack of a Safety Fundamental in safety

Problems in communication caused one of the biggest accidents in aviation i.e. the runway accident on Tenerife. Another example could be the Linate runway incursion that occurred in part because of the ground controller's failure to challenge an incomplete read-back and to clarify unclear position reports from the aircraft. The Linate and Charles de Gaulle runway incursions both involved clearances to other aircraft in local languages. The Charles de Gaulle and Detroit runway incursions both involved inadequate communications between ground and runway controllers. In the Überlingen collision, the controller was distracted in part because of failure of telephone communication with Friedrichshafen, and a warning was not received in part because the telephone from Karlsruhe ACC was inoperative.

The Safety Fundamental as a regulatory requirement

Communication is an essential element of aviation safety and consequently leads to regulatory requirements on standard phraseology (e.g. EC, 2006) as well as requirements on communication means (e.g. ICAO, 2005).

Equally to the Safety Fundamental Organization, the Safety Fundamental Communication relates to the group of Safety Fundamentals on safety management as well (see section 3.2).

3.3.7 Reliability

The definition of the Safety Fundamental

Reliability is defined as the overall safety performance, including the potential of recovering from unwanted situations or failures in time

Guiding questions are; Is a failure controllable by human interventions? How would a human be able to cope with undesired outcomes of the system? Would there be enough time and resources to compensate for failures?

The detailed rationale behind the Safety Fundamental

Reliability is an overall view on operational safety combining all elements of the entire safety performance. It describes the potential to perform safely in a stable manner without breakdowns or service interruptions.

Key to reliability is the concept of resilience, which is the degree to which the overall system design, in all given circumstances or constraints, empowers the user, with his experiences and habits, to maintain the required level of service comparable to normal conditions.

An additional key to reliability is the level of coupling between the various aspects of the system respectively the fault tolerance of the system, individual components or functions. In tightly coupled systems, there is a high interdependency between failures within one part of the overall system, which may lead to the breakdown of a large portion of the overall system. In loosely coupled systems, failures are likely not to propagate as much through the overall system.

A third aspect is the robustness of the system. A robust system will detect and respond appropriately to violations of expected system behaviour within the assumptions about the environment in which it behaves.

Reliability includes three phases: prevention, detection (identification of breakdowns) and recovery (mitigation);

- Prevention – ability to maintain service and prevent unwanted results,
- Detection – the ability to clearly identify the event of failure, even after long periods without service interruption,

- Recoverability – the ability to put the system back into a safe mode, e.g. by temporarily switching to alternative inputs or alternative procedures.

Redundancy is one way of achieving reliability, but non-redundant systems can achieve high levels of reliability in other ways, such as careful design, manufacture and in-service inspection and preventive maintenance.

The manifestations for the lack of a Safety Fundamental in safety

Many aviation accidents relate to the concept of human errors, and "workload" is often given as a cause for human error. The true cause is often much more a complex interrelation of the human and technical part of the man-machine system. A main issue of the technical part is automation. The safety importance of human automation relationships is widely known in safety (Bainbridge, 1987).

The Strasbourg A320 accident on 20th January 1992 is a well investigated automation assisted accident. In addition, the accident with an Airbus A320-211 Aircraft in Warsaw on 14th September 1993 is known as an automated assisted accident. The aircraft was landing under windshear conditions, which - by design - were interlocking the braking systems. ATM does, so far, not suffer from automated assisted accidents but with the envisaged and aspired increase of automation (e.g. by the SESAR concepts), this Safety Fundamental will rise in its importance also for ATM.

The Safety Fundamental as a regulatory requirement

Human automation issues may lead to increased interdependencies or decreased redundancies. Risk assessments that do not consider this interrelation may lead to an underestimation of the risk, in particular in combination with the Safety Fundamentals on interdependence and redundancy (NRC, 2009; IAEA-50, 1992; IAEA NS-G-1.2, 2001; HSK, 2001). The need for considering human automation issues will increasingly become an essential activity in safety regulatory oversight.

Besides human automation issues, this fundamental highlights the importance to have an overarching view on technology, organisation, procedures and human elements in order to have a proper safety oversight opinion about the safety status of an organisation. This opinion needs to be based on a properly combined view on all elements (including their interdependencies) for evaluation of the hazards and needs to evaluate risk in nominal as well as extraordinary situations. Only a total system approach would allow for appropriate risk mitigation and would ensure effective monitoring or verifying of actual risks in a system (NLR SAFMAC, 2007).

Such an safety approach is called a total system approach and is an important aspect of safety regulatory oversight throughout safety relevant industries (DGTREN, 2007) and throughout the life cycle of a system. For instance the safety of a new concept can be validated at pan-European level during the development phase, while the existence of proper procedures applied by trained staff under responsibility of a suitable organisation has to be verified, and be subjected to continuous oversight, at a local level.

3.4 Safety Fundamentals for Safety Performance – Safety Architecture and Technology

Figure 5 outlines the set of Safety Fundamentals on safety performance with respect to safety architecture. The Safety Fundamentals are a cybernetic view and herewith independent of the nature of a system. The system can be of a technological, human, or procedural nature or may contain a combination of all these elements. Any system has an input and an output, some internal functions, and is related to another adjacent system.

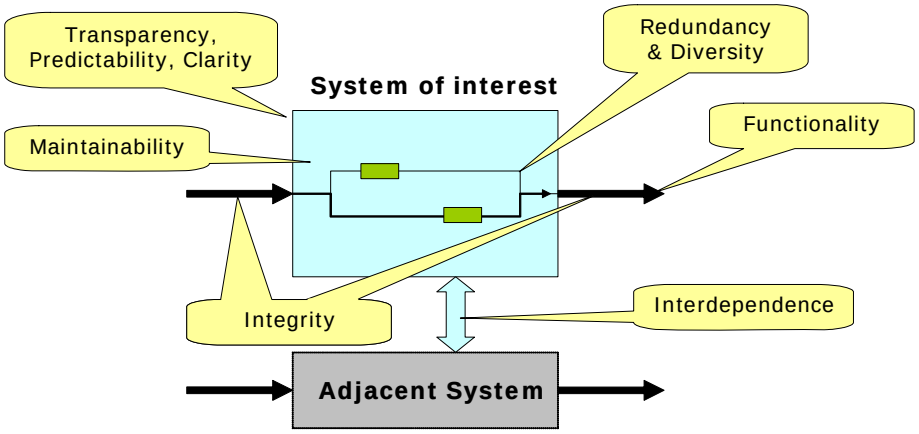

Figure 5: Safety Architecture and Technology perspective

3.4.1 Transparency

The definition of the Safety Fundamental

Transparency describes the ability to specify clearly, what the system is intended to do, and to perform consistently as specified. Transparency therefore is strongly linked to predictability and clarity. From the safety regulatory point of view this includes a clear identification of the legal responsibilities (e.g. of the Galileo designer as distinct from the service provider of the Galileo signal in space).

Guiding questions are; How complete is the design? Is it clearly understandable and unambiguous? Are the specifications well outlined? Is it considered as correct? Which responsibilities will the designer maintain throughout the life cycle?

The detailed rationale behind the Safety Fundamental

Transparency is a widely considered Safety Fundamental for safety. From the safety regulatory viewpoint, it is essential to have confidence that the system and intended changes to the system are clearly understood and that justifications for change are traceable in order to understand the impact on existing safety mechanisms.

Typical problems for safety regulatory acceptance are found in the early phases of changes, where initial regulatory decisions need to be taken. In the nuclear industry this would for instance be the decision for the location of a new plant. In ATM, this might for example be for the principle decision to develop airborne separation capabilities. In this context it is of particular relevance that the SESAR concept at pan-European level during the conceptual development is validated before industry starts designing specific products or software.

If the design is not transparent and cannot be explained clearly, the competent safety oversight authority needs to highlight the need for clarity in order to avoid running the risk of too early acceptance of a proposed design.

Transparency hence implies a clear and explicit identification of the transactions at the interface with the competent safety oversight authority, starting from the development phase.

The manifestations for the lack of a Safety Fundamental in safety

Lack of transparency leads to lack of knowledge about the design and behaviour as well as ambiguity on its functions and potential operational context and herewith to the lack of traceability of the safety performance, or lack of clearly defined legal responsibilities.

In later stages of safety regulatory approval, lack of transparency usually manifests in high uncertainties and in many assumptions in the risk model. In safety cases, this turns out as an incomplete representation of the risk contribution or in an uncertainty of the assessment. In the end this translates in additional time, cost and effort, as demonstrated by the EGNOS programme, launched in the mid-90s, when the concepts contained in the present paper had not yet been developed.

Because of lack in transparency, one important requirement for safety assessments is to address the uncertainties in the assessment and to use adequate methodologies. For instance US-Nuclear Regulatory Commission regulatory guide for using probabilistic risk assessment states (NRC, 2009):

“Consistency with the defence-in-depth philosophy is maintained if:

- A reasonable balance is preserved among prevention of core damage, prevention of containment failure, and consequence mitigation.
- Over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided.
- Redundancy, independence, and diversity are preserved commensurate with the expected frequency, consequences of challenges and uncertainties (e.g., no risk outliers).
- Defences against potential common cause failures are preserved, and the potential for the introduction of new common cause failure mechanisms is assessed.
- Independence of barriers is not degraded.
- Defences against human errors are preserved.
- The intent of the General Design Criteria … is maintained.”

Besides increased effort in risk assessment, using arbitrary assumptions for risk assessments or having a high effort in building the risk model, lack of transparency also leads to high potential of design errors. Design errors may be defined as a feature of a design that makes the system unable to perform according to its specification under some circumstances. Consequently, one cannot assume that all requirements are included in the specification either by explicit reference, or by implicitly referring to an existing standard.

Specifications may contain errors, which promulgate from designer to purchaser to management and eventually to operation. Accordingly, such errors usually become apparent late in the product phase; long time after the initial error was made. Leading authors in safety therefore conclude that “operational errors” are symptoms for preceding malfunctions of the overall system rather than errors on the operational level (e.g. Hollnagel, 2004, Leveson, 2002).

When tracing back operational events or occurrences, usually design deficiencies can be identified. Typical examples that are found when tracing back are bad design of procedures, shortcomings in the compatibility of a system with other systems, quick fixes in user manuals or similar.

The Safety Fundamental as a regulatory requirement

As most of the issues related to transparency could be traced back to the way essential decisions were made in organizations, the requirements for transparency can usually be found in any regulation for Safety-Management-Systems.

The need for striving for transparency is a need identified in safety critical environments. Transparency is explicitly mentioned as key for a Safety-Management-System that meets high safety culture (IAEA INSAG 13, 1999). Any process description required in safety management is a means to make decisions traceable. This also holds for managerial decisions (BMU, 2009). In addition, ICAO-SMM (2007) is highlighting the need for safety culture. The effect of lack of transparency for the assumptions in risk assessments also led to safety regulatory requirements to undertake uncertainty calculations in risk assessments in nuclear (NRC, 2009; IAEA-50, 1992; IAEA NS-G-1.2, 2001; HSK, 2001).

3.4.2 Redundancy

The definition of the Safety Fundamental

Redundancy is defined as the use of independent components performing the same function, protecting the total system against breakdown due to single component failures (single point of failure). In turn these independent components can be based on the same technology (e.g. duplicated engines or duplicated ILS transmitters) or on dissimilar technologies (e.g. radar plus ADS or line-of-sight data link plus satellite data link). From the safety regulatory point of view some responsibilities (e.g. decisions on obligations to equip address to both air operators and ANSPs, or protection of the aeronautical frequency bands or of the aerodrome surroundings) belong to governmental prerogatives, either at national or EU level.

Guiding questions are; does the overall system still have enough “budget” to compensate for reduced performance? Are other (diverse) means established in case of failure? Are the relationships between developers, governments and safety authorities clearly defined?

The detailed rationale behind the Safety Fundamental

Redundancy is one of the main methods of achieving high reliability. It is a key feature of safety design because any system needs to have capabilities to tolerate a failure of an individual constituent, either by an adequate additional or backup function. The use of independent components in parallel protects the system against breakdown due to single component failures. An instance of redundancy is diversity, which means that the same function is fulfilled by a different technical solution.

Redundancy is expressed in factors of safety (e.g. having two engines on an aircraft but the aircraft can still fly and land with one of them, the aircraft engine safety has a factor 2). Safety factors can be in between 1 and 2 (e.g. 1,5 factor safety if the backup function only has 50% of the functionality of the main function). Safety factors can also range up to 4 or 6 if the functions are essential (e.g. power supplies) or have a bad safety performance (in early times only aircraft with four engines were allowed for long distance journeys). From the quantitative risk perspective, the safety factor means a reduction of accident risk (e.g. 1/2 of the risk for a loss of an aircraft due to engine failure).

As an example, the discussion of having a single-pilot cockpit is from a safety perspective a discussion on the reduction of redundancy (in this case human redundancy). The same holds for the reduction of staff in operational control (e.g. one multi sector planner with 3 executive controllers instead of 3 planners and 3 executive controllers).

Redundancy is needed to cover uncertainties due to all possible impacts and to make the system robust / resilient against operational uncertainties, which could not be anticipated in the design.

The manifestations for the lack of a Safety Fundamental in safety

Lack of redundancy is leading to a reduced safety budget. Any lack of redundancy may lead to decreased overall safety performance and bears the potential for a single point of failure. In a fault-tree approach, this would be equivalent to a missing AND gate, and hence affect the reliability of the overall system directly and considerably.

One particular safety issue is that reduced redundancy makes a system more vulnerable to latent errors, usually stemming from preceding errors in design and development or maintenance. Latent errors are errors "sleeping" within the system until they are triggered by certain conditions in operation. A redundant system would allow a second opportunity to recover from latent failures.

An example is the Charles de Gaulle runway incursion (25th May 2000) where the controller's use of the French language for take-off clearance to a French pilot removed a level of redundancy provided by the other aircraft monitoring the tower frequency. The situational awareness of the crew of the other aircraft was reduced, as the crew did not speak French.

On the other side, complex integrated ANS systems are usually originated by the subsequent inclusion of new constituents, contracted in different times by different manufacturers. In order to avoid excessive cost for airspace users (e.g. excessive satellite redundancy, since the availability of line-of-sight radiotelephony had not been considered), the processes and responsibilities to establish the minimum necessary redundancy have to be established.

The Safety Fundamental as a regulatory requirement

A competent safety oversight authority needs to have a clear picture of whether a change is reducing the safety factor and decreasing redundancy or whether adequate countermeasures are considered in order to maintain the safety performance (e.g. additional backup mechanisms). Acceptance of reduced redundancy needs to undergo careful safety regulatory consideration (DOD, 2000; FAA, 2000).

In the nuclear industry, the single point of failure is a strict deterministic requirement (IAEA NS-R-1, 2000). The same principle is applied to airworthiness of aircraft. But in ATM/ANS the presence of dissimilar technologies operational in the same airspace (or on-board) has to be always considered.

3.4.3 Interdependence

The definition of the Safety Fundamental

Interdependence is defined as the degree to which the system interacts in an (un-) intended manner with other systems (which may result e.g. in common cause failures or propagation of errors into adjacent systems).

Guiding questions are: How much is the system performance depending on good performance of other systems? Vice versa, it is equally important to consider how much the system in question does affect the performance of other systems.

The detailed rationale behind the Safety Fundamental

The more complex a total system becomes, the more the originally independently planned elements are likely to become interdependent, for instance due to common methods, procedures, technologies or human aspects.

Interdependencies are considered as the most critical aspects in safety. Hazards can arise from dependent events. Foreseen safety mechanisms could be bypassed or envisaged redundancies can become ineffective. In other words, interdependencies might lead to safety barriers not functioning well.

Classical examples are two independent data processors with both having only the same energy supply. The redundancy in the processors is illusory because there is a common hazard in the power supply. Failures due to common hazards are called common cause or common mode failures. Therefore for ATM/ANS safety critical elements, or for safety critical aerodrome equipments, not only their inherent safety has to be verified, but also the installation/integration on the site.

Interdependencies can be manifold. They can include technical interdependencies (e.g. power supply chain), software dependencies (e.g. a core routine in an operating system affects all dependent functions), human dependencies in operational tasks (e.g. read-back hear-back dependencies), interdependencies in an organization (e.g. management-decisions on cost cutting), or interdependencies between two or more organizations (airlines, service provider and airport operator). However, in a socio-technical system like ATM with many interdependencies on operational, managerial and technical level, the analysis of common mode failures remains to date largely judgmental (IANS, 2009).

As an example, all cases where aircraft-derived data is used by ground-based ATM systems (e.g. SSR-codes) introduce the potential for common-cause failures of safety nets both in the aircraft and on the ground. An example is the Aero Peru crash (2nd October 1996) where pitot-static tube blockage resulted in incorrect altitude indications to both pilot and ATCO.

Independence is not necessarily desirable, as it can result in duplication of services, which is inefficient from an economic perspective. Hence, it may be necessary to accept a degree of interdependence as part of an efficient design. In other words, the safety design objective of independence will at some point lead to a trade-off with the design objective of efficiency. The key issue here is to come to an argument that the safety of the total system is still sufficiently managed. A typical case for consideration is ADS using satellite positioning as source information.

The manifestations for the lack of a Safety Fundamental in safety

Interdependencies result to the existence of common causes in safety assessments. If common causes are not effectively modelled in a safety assessment, it leads to a potential underestimation of the risk. Interdependencies may well make “nonsense out of quantitative calculations” in risk assessment. Evidence shows that they cause a high proportion of failures. In the nuclear industry, where a lot of experience was generated using quantitative risk assessment the portion of interdependencies amounts up to about 80% of the overall risk of the system.

Hence quantitative risk assessment methods not providing techniques to address interdependencies lead to arbitrary results. Consequently, there should be a requirement to fully address the issue of interdependencies fully in quantitative risk assessment if the results are to be used for any managerial or safety regulatory decision.

The Safety Fundamental as a regulatory requirement

In the nuclear industry, there is a long tradition in dealing with interdependencies (NRC, 2009; BFS, 2004). This tradition is built on lessons learned from some severe incidents and accidents, as the industry was initially too much relying on Risk Based Regulation. Risk based regulation comprises a safety regulatory approach where the regulator bases the decisions purely on the assessed risk.

As - per definition - unknown dependencies cannot be represented in such an approach, the nuclear industry shifted towards risk Informed Decision Regulation, i.e. quantitative risk assessment was no more seen as the sole criterion but one of many other means to ensure safety (OECD, 2008).

The functional ATM system is highly interdependent and - taking the above into consideration - it requires more than any other industry to look into interdependencies in risk assessment approaches (e.g. ESARR 6, 2003; IAEA NS-R-1, 2000). In particular ATM is interdependent with other parts of the total aviation system, as well known for instance in the case of runway incursions or excursions, whose causal factors are usually scattered across different aviation domains.

3.4.4 Functionality

The definition of the Safety Fundamental

Functionality is defined as the correctness, consistency and un-ambiguity of the behaviour of the system.

Guiding questions are; Is the required functionality clearly specified? Does the system provide its specified functionality under all circumstances? Are there external circumstances where the system performance would not be guaranteed? Is the system able to flexible reactions (or "to flexibly react) on changes of its input or environment?

The detailed rationale behind the Safety Fundamental

Functionality describes how well a system is able to deliver in design-based situations as well as in beyond design-based situations. For example, many accidents result from inadequate functionality of safety equipment: the Linate runway collision (8th October 2001) was in part caused by a lack of runway guard lights and controllable stop bars. In some accidents, safety equipment fails to make its intended contribution to preventing accidents like in the Überlingen mid-air collision (1st July 2002), which was partly caused by incorrect use of ACAS.

The manifestations for the lack of a Safety Fundamental in safety

Latent errors are often the consequence of lack of functionality of a sub-system, in particular if the system operates in challenging or beyond-design situations. Those situations are the missing elements in modelling the system safety and hence affect the representativeness or completeness of a safety assessment. Lack of functionality may result in a lack of inherent safety-features.

The Safety Fundamental as a regulatory requirement

In nuclear regulation, there is a strict distinction between design based- situations (nominal risk situations) and beyond design-based situations. Design-based situations are those situations anticipated by the designer, where specific means are provided to manage these situations safely e.g. using barriers (INSAG 12, 1999).

Beyond design-based situations are those situations which are not anticipated by the designer, where general means need to be in place to manage these situations safely, e.g. by establishing emergency plans (IAEA NS-R-1, 2000).

A key function of safety regulatory approval and ongoing oversight is to verify whether a design is able to cope with all situations known at the time of approval (e.g. whether an aircraft is able to cope with all known adverse weather conditions). Indications at early stages of development and proof at the earliest possible stage should be submitted in the form of evidence or clarification of fail-safe behaviour of operational component modes.

In this context it has to be recalled that validation starts with system development, when technical specifications may not be available or complete: its object is a new concept or technique. Technical specifications are one of the output of development. Vice versa verification refers to a specific design or product versus the applicable specifications.

3.4.5 Integrity

The definition of the Safety Fundamental

Integrity is defined as the trustworthiness of the system outputs, i.e. their freedom from errors given correct input (fail-safe principle; absence of errors of commission).

Guiding questions are: Is the system able to fail in a "fail-safe" mode? Is the system potentially generating outputs, which might be harmful?

The detailed rationale behind the Safety Fundamental

Integrity highlights errors or malfunction from input to output processing, which may result into breakdowns. The issue is well known for data processing (e.g. Flight Data Processing Systems). This Safety Fundamental is expected to have higher importance in any future ATM system, as this is expected to progressively become fully reliant on shared data and hence on integrity of data processing (e.g. due to changes like data-link or satellite based navigation).

The manifestations for the lack of a Safety Fundamental in safety

Lack in integrity may result in unintended outcomes, which are called errors of commission in safety assessments (i.e. the performance is in an unanticipated manner related to the input information). Errors of commission are difficult to model and hence usually not considered in safety assessments (e.g. software reliability but also human reliability). Consequently, analytical or probabilistic risk assessments might underestimate the risk.

The Cali CFIT (20th December 1995) was in part attributed to FMS-generated navigational information using a different naming convention from the published navigational charts. The St Louis runway incursion (22nd November 1994) was in part due to ATIS not mentioning the runway which the light aircraft was cleared for. These are both types of integrity failures.

The Safety Fundamental as a regulatory requirement

A key function of safety regulatory approval and ongoing oversight is to verify the integrity and to check whether the design is able to cope with all known situations (IAEA NS-R-1, 2000; IEC 62278, 2002).

An important principle of safety oversight is to ask for fail-safe behaviour if the integrity is in question (e.g. if invalid input data needs to be processed).

3.4.6 Maintainability

The definition of the Safety Fundamental

Maintainability is defined as the ability to maintain the system in working order throughout its life. This includes preventive maintainability, on-line maintenance, and reparability. From the safety regulatory point of view it includes defining which organisations and which persons have the privilege of maintaining the system in, or returning the system to service. This scope is totally sufficient for the aircraft case as maintenance takes place when the aircraft is not flying. In ATM/ANS, additionally, the systems may be maintained or re-configured during real-time operations without interruption of service. This latter aspect has to be considered in addition in ATM/ANS.

Guiding questions are; how much is the system performance depending on the activities required to maintain the system? How recognizable is a potential error in maintenance?

The detailed rationale behind the Safety Fundamental

The ability to maintain the system in working order throughout its life includes:

- Preventive maintainability - ability to inspect, detect and correct incipient (i.e. early-stage) failures before they result in actual failures, without degrading safety or introducing latent (i.e. dormant) failures. Including preventive maintenance on systems which are in operational use.
- On-line maintenance – the ability to inspect, detect and correct incipient failures without interrupting the operation.
- Corrective maintainability (reparability) - ability to reconfigure a system in real time after a failure ("graceful degradation") and ability to repair the system to the original state after a failure has occurred.

The manifestations for the lack of a Safety Fundamental in safety

Maintainability is an often forgotten aspect in design. Once the system is implemented, it is discovered that essential feedback for detection of malfunctions is missing or updates can only be made in a very complicated manner (e.g. software update that requires restart of the entire system).

In combination with reliability, maintainability determines the overall availability of a system, which is one of the Safety Fundamental measures of the degree of protection against breakdowns.

Many aviation accidents have resulted from deficiencies in maintenance. For example, the Linate runway incursion (8th October 2001) was in part attributable to the failure to maintain the airport surface movement indicator (ASMI). The Überlingen mid-air collision (1st July 2002) was partly due to on-line maintenance of STCA and telephone lines. Competence of the related personnel, beyond strictly technical tasks, is therefore one of the key issues.

The Safety Fundamental as a regulatory requirement

Lack in Maintainability has proven to contribute to a high potential of latent errors. Latent errors are difficult to identify and often not represented in safety assessments, which may consequently lead to an underestimation of risk (IEC 300-3, 1995; VDI 4003, 2007; API 2000, 2009).

Due to this, the safety regulatory ongoing oversight is essential to function as an additional means to identify latent errors or to balance the risk assessment.

4. CONCLUSIONS

This document provides a concise description of Safety Fundamentals. The Safety Fundamentals were derived from a range of existing safety regulations and structured according to cybernetic considerations. Any argumentation about the needs for a Safety Fundamental – besides those regarding naming or terminology - would mean arguing on existing safety regulations or their validity for ATM.

Safety Fundamentals exist in any industry. The Safety Fundamentals are not a new invention but reflect existing requirements and standards that are the basis of regulatory tasks in a consistent framework. In nuclear they are seen as the top-level requirements for any nuclear installation worldwide (IAEA, 2006).

This report evaluates a range of requirements form different industries in order to provide a synopsis of the available safety regulatory requirements. Many of the mentioned requirements stem from nuclear industry. The reason might be that this industry is in the particular situation to be obliged – due to the enormous consequences of an accident - to request a zero-accident regulatory policy. Nevertheless the derived Safety Fundamentals are equally applicable to ATM and aviation in general because both nuclear and aviation are systems which consist of the combination of human aspects, procedural aspects and technology. As nuclear is mainly a technology-driven system while aviation is more a human and procedural driven system, one can even conclude that in particular the operational and managerial Safety Fundamentals are of even higher importance for safety in aviation as they are for nuclear.

Safety Fundamentals provide a framework for safety regulatory oversight or for decision-making about the impact of changes on the safety regulatory responsibilities. These need a good understanding of safety concerns and potential issues and besides a proper competence of the safety oversight authorities, there needs to be a complete consideration of where safety requirements are potentially violated by a change or new design.

Therefore, the aim of the use of Safety Fundamentals is not to question the currently existing safety regulatory framework either captured in SES or ESARRs but is rather aiming at a structured approach to discuss/scan a development looking from a safety perspective using the Safety Fundamentals (as essential criteria for a safe design) for the discussion. When coming to the area of the regulatory framework as such the scanning could identify the need for new regulatory requirements (e.g. equipment certification or needs for human licensing) or possibly the identification of the need to revisit or expand existing legislation (e.g. when ICAO does not capture a development in the Annexes or SARPS then the need to do so can be identified). The scanning ends at the point of raising the issue (i.e. the consideration) and would allow the clarification who should do it (e.g. Global, pan-European or national legislators). These rulemaking processes as such are outside the scope of the scanning.

The summarizing Table 1 below comprises the regulatory requirement stemming from a range of different industries and the Safety Fundamental.

(Space Left Intentionally Blank)

Table 1 – Overview of the Safety Fundamentals and their Basis in Safety Regulations Based on a Selection of Existing Safety Regulations in Safety-Critical Domains

Regulatory Requirement		Safety Fundamental
Safety Performance - Safety Architecture and Technology		
BMU, 2009 HSK, 2001 IAEA INSAG 13, 1999 IAEA NS-G-1.2, 2001	IAEA-50, 1992 ICAO-SMM, 2007 NRC, 2009	Transparency
FAA, 2000 IAEA NS-R-1, 2000	DOD, 2000	Redundancy
IAEA NS-R-1, 2000 ESARR 6, 2003	BFS, 2004	Interdependence
INSAG 12, 1999 IAEA NS-R-1, 2000		Functionality
IAEA NS-R-1, 2000 IEC 62278, 2002		Integrity
IEC 300-3, 1995 VDI 4003, 2007	API 2000, 2009	Maintainability
Safety Performance - Operational Safety Aspects		
IAEA NS-R-2, 2000 ESARR 5, 2005;	EC, 2006	Procedures
IAEA, 2005 WENRA 2003	IAEA NS G2.8, 2002 ICAO Annex 1, 2009	Competence
FAA, 2009 ICAO Doc 9683		Human-machine interaction
IAEA NS-R-2, 2000 IAEA SG-Q, 1996		Operating Environment
ICAO-SMM, 2007 IAEA DS 338, 2005	IAEA INSAG13, 1999 OECD, 2008	Organization
EC, 2006 ICAO, 2005	IAEA NS-G 2.4, 2001	Communication
NRC, 2009 IAEA-50, 1992	IAEA NS-G-1.2, 2001 HSK, 2001	Reliability
Safety Management		
IAEA INSAG 13, 1999 ICAO-SMM, 2007	BMU, 2008 DGTREN, 2007	Understanding and Openness
ESARR 1, 2004 IAEA INSAG 13, 1999	BMU, 2009 ISO 60300, 2007	Completeness and Freedom from bias
INSAG 13, 1999 IAEA SG-Q, 1996	ESARR 1, 2004	Responsibility and Practicability
ICAO-SMM, 2007 IAEA/NEA 1998	DG TREN, 2007 ESARR 1, 2004	Detectability and Feedback
IAEA, 2006 RSK, 2008	BFS, 2004	Responsiveness and Learning
Safety Regulation - Basic principles of Safety Regulation		
BMU, 2009 ICAO SMM, 2007	ISO 9001, 2000 IAEA SG-Q, 1996	Responsibility for Safety
EC, 1985 ICAO SMM, 2007	IAEA, 2006	Ensure safety standard
ESARR1, 2004 EC, 2007	ICAO, 2007 IAEA, 2006	Independent oversight

Applications of the Safety Fundamentals outlined above exist for the SESAR Definition phase, for operational concept development for airports, and for safety in other transportation areas (Rail). The way Safety Fundamentals are applied is in fact close to the way the EFQM model works, which provides high-level requirements for important parameters for quality (EFQM, 2009). Therefore Safety Fundamentals could be used to provide the basis of the safety perspective in an integrated Management-System where safety perspectives need to be aligned with other performance parameter.

Safety Fundamentals are flexible to be adapted to new safety thinking or additional fundamentals could be included. Some Safety Fundamentals might be split up in the future to make their underlying aspects more explicit. As an example, the current definition of reliability comprises three concepts: resilience, degree of coupling within a system and robustness. Recently, resilience became an important aspect for safety. It may be transformed into a first order Safety Fundamental. In addition, the distinction between high cohesion and low coupling might be worth making it a separate Safety Fundamental. However, such rearrangements would ultimately refine but not question the approach of Safety Fundamentals.

Other Safety Fundamentals could be integrated on a higher level of abstraction if so desired (e.g. the openness, understanding, completeness, and freedom from bias could be aggregated to the general term safety culture). However, this term then would need the Safety Fundamentals as explanation.

5. REFERENCES

5.1 References to Related Deliverables for the Development of the Safety Scanning Tool

- SCAN TF (2010, SST questions) – SCAN Task Force, Development of a Set of Questions for the Safety Scanning Tool, Edition 1.0, 11 March 2010, M.H.C. Everdij, H. Korteweg, J. Penny, O. Straeter, T. Longhurst.
- SCAN TF (2010, SST) – SCAN Task Force, Safety Scanning Tool, Excel-based Tool, 11 March 2010, A. Burrage, O. Straeter, M.H.C. Everdij.
- SCAN TF (2011, SMRT questions) – SCAN Task Force, Development of a Set of Questions for the Safety Methods Review Tool, Edition 1.1, 11 April 2011, M.H.C. Everdij, O. Straeter, J.W. Nollet, H. Korteweg.
- SCAN TF (2010, SMRT) – SCAN Task Force, Safety Methods Review Tool, Excel-based Tool, 11 March 2010, A. Burrage, M.H.C. Everdij.
- SCAN TF (2011, multi actor) – SCAN Task Force, Safety scanning as part of the oversight process, version 1.0, 26 May 2011, H. Korteweg, O. Straeter, J.W. Nollet, M.A. Kraan.
- SRC DOC 46 – Annex B, moderating – SCAN Task Force, Guidance for moderating a Safety scanning event.
- SRC DOC 46 – Annex C, interpreting – SCAN Task Force, Guidance on Interpreting and Using the Safety scanning results.
- SRC DOC – Annex D, regulatory advice – SCAN Task Force, Supporting Regulatory Tasks with Safety scanning.

5.2 References to Safety Regulations or Standards Demonstrating the Structure and Use of Safety Fundamentals

- API 2000 (2009) Venting Atmospheric and Low Pressure Storage Tanks - Nonrefrigerated and Refrigerated. American Petroleum Institute. Washington.
- BFS (2004) Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Facharbeitskreis ”Probabilistische Sicherheitsanalyse für Kernkraftwerke”. BFS. Salzgitter.
- BMU (2009) Modul 8 Sicherheitskriterien für Kernkraftwerke: Kriterien für das Management der Sicherheit. Bundesministerium für Umwelt und Reaktorsicherheit. Bonn.
- DGTREN (2007) “Regulation and enforcement in aviation, shipping and nuclear industries-What could we learn from each other?”. Workshop proceedings. DGTREN. Luxembourg
- DIN EN ISO 14001 (2005) Environmental management systems - Requirements with guidance for use. ISO. Geneva.
- DOD (2000). Standard Practice for System Safety. Washington, DC, USA: U.S. Department of Defense. MIL-STD-822D.
- EC (1985) Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products
- EC (2005) COMMISSION REGULATION (EC) No 2096/2005 of 20 December 2005 laying down common requirements for the provision of air navigation services
- EC (2006) Directive 2006/23/EC OF The European Parliament And Of The Council of 5 April 2006 on a Community air traffic controller licence
- EC (2007) COMMISSION REGULATION (EC) No 1315/2007 of 8 November 2007on safety oversight in air traffic management and amending Regulation (EC) No 2096/2005
- EFQM (2009) EFQM-Model. European Foundation for Quality Management.
- ESARR 1 (2004) ESARR 1 - Safety Oversight IN ATM, edition 1.0, 05 November 2004
- ESARR 2 (2000) ESARR 2 - Reporting and Assessment of Safety Occurrences in ATM. Eurocontrol. Brussels.
- ESARR 3 (2000) ESARR 3 - Use of Safety Management Systems by ATM Service Providers. Eurocontrol. Brussels.
- ESARR 4 (2001) ESARR 4 - Risk Assessment and Mitigation in ATM. Eurocontrol. Brussels.
- ESARR 5 (2005) ESARR 5 - ATM Services' Personnel. Eurocontrol. Brussels.
- ESARR 6 (2003) ESARR 6 - Software in ATM Systems. Eurocontrol. Brussels.
- FAA (2000). System Safety Handbook. Washington, DC, USA: U.S. Federal Aviation Administration (FAA).
- FAA (2009) Human Factor Design Guide. FAA. Washington
- HSK (2000) Guidelines for the regulatory Review on Human Reliability Analysis in PSA (HSK-AN-3584). HSK. Switzerland.
- HSK (2001) Periodische Sicherheitsüberprüfung von Kernkraftwerken. HSK R 48. HSK. Vilingen-HSK / Schweiz.

- IAEA (1988) Safety Series - Basic Principles for Nuclear Power Plants. IAEA. Vienna.
- IAEA (1989) Systems for Reporting Unusual Events in Nuclear Power Plants. IAEA Safety Series No. 93. Vienna.
- IAEA (1991) Safety Culture. Safety Series No. 75-INSAG-4, IAEA, Vienna, Austria
- [IAEA (1992) Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1). Safety Series No. 50 P. IAEA. Vienna. p. 51 ff.
- IAEA (1995) Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants. Safety Series No. 50 P 10. IAEA. Vienna.
- IAEA (1996) The Management System for Facilities and Activities. IAEA SAFETY STANDARDS. DS338. IAEA. Vienna.
- IAEA (2005) SAFETY STANDARDS for protecting people and the environment - The Management System for Facilities and Activities. DS338 Draft 10 - Revision of Safety Series 50-C-Q (1996). International Atomic Energy Agency. Vienna.
- IAEA (2006) Fundamental Safety Principles IAEA Safety Standards Series No. SF-1. IAEA Vienna.
- IAEA (2006) The Management System for Facilities and Activities Safety Requirements. Safety Standards Series No. GS-R-3. IAEA. Vienna.JAR-FCL 1, 2 and 3 requirements
- IAEA DS 338 (2005) Safety Standards for protecting people and the environment - The Management System for Facilities and Activities. DS338 Draft 10 - Revision of Safety Series 50-C-Q (1996). International Atomic Energy Agency. Vienna.
- IAEA GS-R-3 (2006) The Management System for Facilities and Activities. IAEA Vienna.
- IAEA INSAG 12 (1999) Basic safety principles For nuclear power plants. 75-INSAG-3 rev. IAEA Vienna.
- IAEA INSAG 13 (1999) Management of Operational Safety in Nuclear Power Plants. IAEA Vienna.
- IAEA NS-G-1.2 (2001) Safety Assessment and Verification for Nuclear Power Plants. IAEA. Vienna.
- IAEA NS-G-2.4 (2001) IAEA The Operating Organization for Nuclear Power Plants. Safety Standard. IAEA. Vienna.
- IAEA NS-G-2.8 (2002) Recruitment, Qualification and Training of Personnel for Nuclear Power Plants. SAFETY GUIDE. IAEA. Vienna.
- IAEA NS-R-1 (2000) Safety of Nuclear Power Plants: Design. IAEA. Vienna.
- IAEA NS-R-2 (2000) Safety of Nuclear Power Plants: Operation. IAEA. Vienna.
- IAEA SG-Q (1996) Quality Assurance for Safety in Nuclear Power Plants and Other Nuclear Installations, Code and Safety Guides Q1–Q14, Safety Series No. 50-C/SGQ, IAEA, Vienna, Austria
- IAEA/NEA (1998) IAEA/NEA Incident reporting System (IRS) Reporting guidelines – Feedback from safety related operating experience from Nuclear Power Plants. IAEA. Vienna.
- IANS (2009) Introduction to Safety Assessment Methodology. Eurocontrol IANS, Luxembourg.
- ICAO (1998) ICAO Doc 9683 Human Factors Training Manual Part I (Basic aviation Human Factors concepts) and Part II (Human Factors training Programmes for operational personnel). ICAO. Montreal. (ISBN 92-9194-090-9)

- ICAO (2001) ICAO Annex 13 to the Convention on International Civil Aviation- Aircraft Accident and Incident Investigation (9th edition). ICAO. Montreal
- ICAO (2005) ICAO Doc 9432 - Manual of Radiotelephony. ICAO. Montreal. (ISBN 92-9194-633-8)
- ICAO Annex 1 (2009) ICAO Annex 1. Personnel Licensing. Ed 10. ICAO. Geneve.
- ICAO Doc 9683 (2009) Human Factors Training Manual. ICAO. Geneve.
- ICAO SMM (2007) Safety Management Manual. ICAO. Geneva
- IEC 300-3 (1995) Dependability Management - Part 3: Application Guide - Section 9: Risk Analysis of Technological Systems
- IEC 62278 (2002) Railway Applications Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
- ISO 60300 (2007). Dependability Mangement. International Organization for Standardization. Geneve, Switzerland.
- ISO 9001:2000 (2000) Quality Management Systems: Requirements. Geneva, Switzerland (2000).
- ISO-DIS 10075 (2002) Ergonomic principles related to mental workload. International Organization for Standardization. Geneve, Switzerland.
- ISO-DIS 9241 (1993) Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs). International Organization for Standardization. Geneve, Switzerland.
- JAR OPS 1.943 CRM-Grundschulung des Luftfahrtunternehmers (Crew Resource Management - effektives Arbeiten als Besatzung)
- NRC (2009) NRC Regulatory Guide 1.174 - An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis.
- OECD (2008) The Regulatory Goal of Assuring Nuclear Safety NEA No. 6273, OECD NEA. Paris. ISBN 978-92-64-99044-9
- RSK (2008) Anforderungen an ganzheitliche Ereignisanalysen. BMU. Bonn.
- VDI (1992) Mit Instrumentenflug in den Tod. VDI-Nachrichten. Nr. 28. VDI. Düsseldorf.
- VDI 4003 (2007) Reliability management. VDI. Duesseldorf.
- VDI 4006 (1999) Menschliche Zuverlässigkeit - Ergonomische Forderungen und Methoden der Bewertung. Beuth-Verlag. Berlin.
- VDI 4006 (2002) Menschliche Zuverlässigkeit - Methoden zur quantitativen Bewertung menschlicher Zuverlässigkeit. Beuth-Verlag. Berlin.
- VDI/VDE 2180 „Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT)“ Teile 1-4, Beuth-Verlag Berlin (2007)
- VROM (2005) Publication Series on Dangerous Substances 4 (PGS 4): Methods for determining and processing probabilities – "Red Book" CPR 12E (1997)
- WENRA (2003) Training and Authorization of NPP staff. Western European Nuclear Regulator Association. 25 September 2003

5.3 References Demonstrating the Structure and Content of Safety Fundamentals

- Bainbridge, L. (1987) The Ironies of Automation. In: Rasmussen, J., Duncan, K. & Leplat, J. (Eds.) New Technology and Human Error. Wiley. London.

- Braband, J. (2004) Risikoakzeptanzkriterien und -bewertungsmethoden - Ein systematischer Vergleich. Signal + Draht, (96) 2004, Heft 4
- Hollnagel, E. (2004) Barriers And Accident Prevention. Ashgate. Aldershot.
- Hollnagel, E., Woods, D. & Leveson, N. (2005) Resilience Engineering - Concepts and Precepts. Ashgate. Aldershot. (ISBN 0754646416)
- IAEA (2000) IRS Study on Incidents Caused by Loss Of Corporate Knowledge And Memory (Phase I - Selection of events for in depth analysis). IAEA. Vienna (IAEA-J4-CS-10/00).
- IAEA (2001) IRS Study on Incidents Caused by Loss Of Corporate Knowledge And Memory (Phase II - In depth analysis of selected events). IAEA. Vienna (IAEA-J4-CS-04/01).
- Leveson, N. (2002) System Safety Engineering: Back To The Future. Massachusetts Institute of Technology. Boston
- OECD-NEA (2004) Proceedings of the Joint CNRA/CSNI Workshop on the regulatory uses of safety performance indicators, Granada, Spain, 12-14 May 2004.
- Perrow, C. (1999) Normal Accidents: Living with High-Risk Technologies. 2. Auflage. Princeton University Press, Princeton, NJ 1984/1999,
- Probst, C. (2007) Regulatory authorities in aviation safety - From National to Community regulation. In: DGTREN “Regulation and enforcement in aviation, shipping and nuclear industries-What could we learn from each other?”. Workshop proceedings. DGTREN. Luxembourg.
- Reason, J. (1976) Absent minds. New Society. Vol. 4. p. 244-245.
- Reason, J. (1990) Human Error. Cambridge University Press. Cambridge.
- Reason, J. (1997) Managing the Risk of Organizational Accidents. Ashgate. Aldershot.
- Roelen, A.L.C., Wever, R. & Verbeek, M. (2003) Improving aviation safety by better understanding and handling of interfaces - A pilot study. NLR-CR-2003, DGL/2.03.82.129. NLR. Amsterdam.
- SESAR JU 16 (2008) WP 16 - R&D Transversal Areas Description of Work (DoW) Version 4.0. SESAR JU. Brussels.
- SESAR JU 4 (2008) WP 4 WP 4 - En Route Operations. SESAR JU. Brussels.
- Tversky, A. & Kahneman, D. (1974) Judgement under Uncertainty: Heuristics and biases. Science, 184. p. 1124-1131.

5.4 References to Documents Making Use of the Safety Fundamentals

- Catriona Richmond, C. Pasquini, A., Vickery, K. (2007) Safety in Cost Benefit Assessment - Proposed Process for linking Safety Fundamentals to Cost Benefit Analysis. Icon Consulting for Eurocontrol.
- EUROCONTROL - Safety Agenda (2005) The Eurocontrol Safety Agenda 2020. Eurocontrol. Brussels.

- EUROCONTROL - Screening (2006) Safety Screening Technique - Version 0.5. Eurocontrol. Brussels.
- EUROCONTROL - Screening (2007) Safety Screening Technique - Version 1.0 Eurocontrol. Brussels.
- Eurocontrol (2007) Safety Screening Technique. A brochure. SESAR & Eurocontrol.
- Eurocontrol EEC (2006) Safety Considerations Booklet. Eurocontrol. Bretigny.
- Everdij, M. & Blom, H. (2006) SAFMAC - Principles of a safety validation framework for major changes in air transport operations, Final report, National Aerospace Laboratory NLR, NLR-CR-2006-359-PT-3, 30 June 2006.
- Everdij, M., Blom, H., Nollet, J.W., Kraan, A.M. (2006) Need for novel approach in aviation safety validation, Proceedings Safety R&D Seminar, Barcelona, Spain, October 2006.
- Everdij, M.H.C., Blom, H.A.P., Scholte, J.J., Nollet, J.W., Kraan, M.A., 'Developing a framework for safety validation of multi-stakeholder changes in air transport operations', Safety Science, Volume 47, Issue 3, March 2009, pages 405-420. doi:10.1016/j.ssi.2008.07.021.
- Everdij, M.H.C., Blom, H.A.P., Study of the quality of safety assessment methodology in air transport, Proceedings 25th International System Safety Conference, Engineering a Safer World, Hosted by the System Safety Society, Baltimore, Maryland USA, 13−17 August 2007, Editors: Ann G. Boyer and Norman J. Gauthier, pages 25−35, 2007.
- Everdij, M., Smeltink, J., Burrage, A., Kovarova, J., Amar, G., Sträter, O. (2007) Developing a Safety Screening Tool for SESAR related Operational Concepts (NLR-CR-2006-680)
- Everdij, M. & Balk, A. (2008) Advancing the Safety Screening Tool with SAFMAC Principles. NLR. Amsterdam (NLR-CR-2007-763)
- Jansen, R.B.H.J., Smeltink, J. (2006). "A Safety Fundamentals method to screen safety issues for future ATM operational concepts", NLR report for Eurocontrol, NLR-CR-2006-267, 2006
- Krastev, A. (2005) Safety Fundamentals for integration of safety into planning. Future Aviation Safety Team 25. 11/12 April 2005, Toulouse
- SESAR (2008) SESAR Safety Register. SESAR Consortium. Toulouse/France
- SESAR Consortium (2006), SESAR Definition Phase ATM Safety Regulation, Vision for the future Regulatory Framework, WP1.6.1/D2, DLT_0607_161_00_04, 2006.
- SESAR-D3 (2007) ATM Safety Regulation - SESAR Safety Screening & SESAR Concept, Institutions and Regulations. SESAR Consortium. Toulouse/France
- Straeter, O. & Kuijper, J. (2005) Safety Fundamentals for integration of safety into planning
- Sträter, O. & Pasquini, A. (2007) SESAR Safety Screening - A resilient approach towards the single European Sky. Resist Summer School. Proquerolles, France
- Sträter, O. (2004) Implementation and Monitoring of the Effectiveness of Safety Management Systems. Approaches and Challenges in Air traffic Control and Nuclear Energy. Sicherheitsmanagement in der Kerntechnik. Symposium 5. – 6. Oktober 2004. München. TÜV Süddeutschland. München.
- Sträter, O. (2004) Responsibilities and Challenges of Human Reliability Assessment in the Regulatory Framework. PSAM 7 2004. Berlin.

- Sträter, O. (2005) Safety Applications to Air Transport. Proceedings of the Thematic Forum on Risk Analysis & Applications to Safety Decisions for Safety Managers. Center for Nuclear Safety in Central and Eastern Europe (CENS) Bratislava, Slovak Republic.
- Sträter, O. (2006) Kulturelle Herausforderungen für ein künftig sicheres Luftfahrtwesen. Internationaler Kongress „Sicherheit im Verkehrswesen 2006“, 15. und 16. März 2006 in Fulda / Germany.
- Sträter, O. (2006) Managing Safety Proactively – Experiences on the Implementation of the Safety Agenda at Eurocontrol. PSAM 8.
- Sträter, O. (2006) The dilemma of ill-defining the safety performance of systems if using a non-resilient safety assessment approach. Eurocontrol Safety R&D Seminar. Barcelona.
- Sträter, O. (2008) Towards a resilient approach of safety assessment - Experiences based on the design of the future Air Traffic Management System. In Hollnagel, E., Nemeth, C. & Dekker, S. (2008) Resilience Engineering Perspectives: Remaining Sensitive to the Possibility of Failure. Ashgate. Aldershot.
- Sträter, O., Everdij, M., Smeltink, J., Nollet, J., Kovarova, J., Korteweg, H., Burrage, A. (2007) Safety Screening - Experiences in applying a proactive approach to concept development within SESAR. Eurocontrol Safety R&D Seminar – Rome.
- Sträter, O., Krastev, A., Grippa, D., Jansen, R., Smeltink, J., Everdij, M., Spouge, J., Salmon, D., Smith, E., Balfanz, H-P., Kuijper, J. (2006) Safety Screening technique, Edition 0.5, 1 March 2006, Final Draft.
- Sträter, O., Leonhardt, J., Durrett, D. & Hartung, J. (2006) The dilemma of ill-defining the safety performance of systems if using a non-resilient safety assessment approach - Experiences based on the design of the future Air Traffic Management System. 2nd Symposium on Resilience Engineering. Nice/France.
- Zotov, D. (2007) Change Safety Screening. Australian Aviation Psychology Association Symposium. Available from Civil Aviation Safety Authority Australia.

(***)