Agenda Item 3: Hazard identification and safety risk management

SAFETY SYSTEM ASSESSMENT PROCESS

(Presented by the Secretariat)

Summary

This working paper presents information on the steps to follow in the safety assessment process for RNAV5 implementation in the South American Region airspace, and the ATS routes network optimisation.

References:

- Doc 9859 – SMM Manual

ICAO Strategic objectives

Strategic Objective A *Safety*
Strategic Objective D *Efficiency*

1 Background

1.1 Safety Management is a means through which organisations could control the processes that could lead to risky events, to ensure that the risk or harm be limited to an acceptable level. Safety assessment, which is one of the main functions of a safety management system, provides a mechanism to identify potential hazards and find ways to control the risk associated to them.

2 Analysis

2.1 The scope of safety assessment must be wide enough to cover all aspects of the ATS system that will be affected by the change, directly or indirectly.

2.2 A safety assessment is based and addressed to provide responses to three main questions:

- What could go wrong?
- Which would be the consequences?
- How often could it happen?

2.3 Safety assessment requires a systematic approach. The whole process may be divided into the following steps:

First step: Elaboration (or obtaining) of a complete description of the system that must be evaluated and the environment in which the system will have to work.
Second step: Hazard identification
Third step: Evaluation of the consequences of a hazard, expressed in terms of probability
Fourth step: Evaluation of the consequences of a hazard, expressed in terms of severity
Fifth step: Risk rate/tolerability
Sixth step: Risk mitigation
Seventh step: elaboration of safety assessment documents.

2.4 A description of each one of the aforementioned steps is shown in **Appendix A** to this working paper.

3 Suggested action

3.1 The Workshop/Seminar is invited to take note of the information provided and review, and take as reference the content of Appendix A to this working paper, for the task to be developed regarding safety for RNAV5 and ATSRO implementation.

APPENDIX A

SAFETY ASSESSMENT PROCESS

1. Safety assessment process may be divided into the following steps described below:

First Step: Elaboration (or obtaining) of a complete description of the system that must be assessed and the environment in which the system will have to work.

Second Step: Hazard identification

Third Step: Evaluation of the consequences of a hazard, expressed in terms of probability

Fourth Step: Evaluation of the consequences of a hazard, expressed in terms of severity

Fifth Step: Risk rate/tolerability

Sixth Step: Risk mitigation

Seventh Step: Elaboration of safety assessment documents.

2. The following figure **Figure 01** shows a diagram which illustrates the safety assessment process, and shows the possible need to carry out several cycles of the process until finding a satisfactory method for risk mitigation.

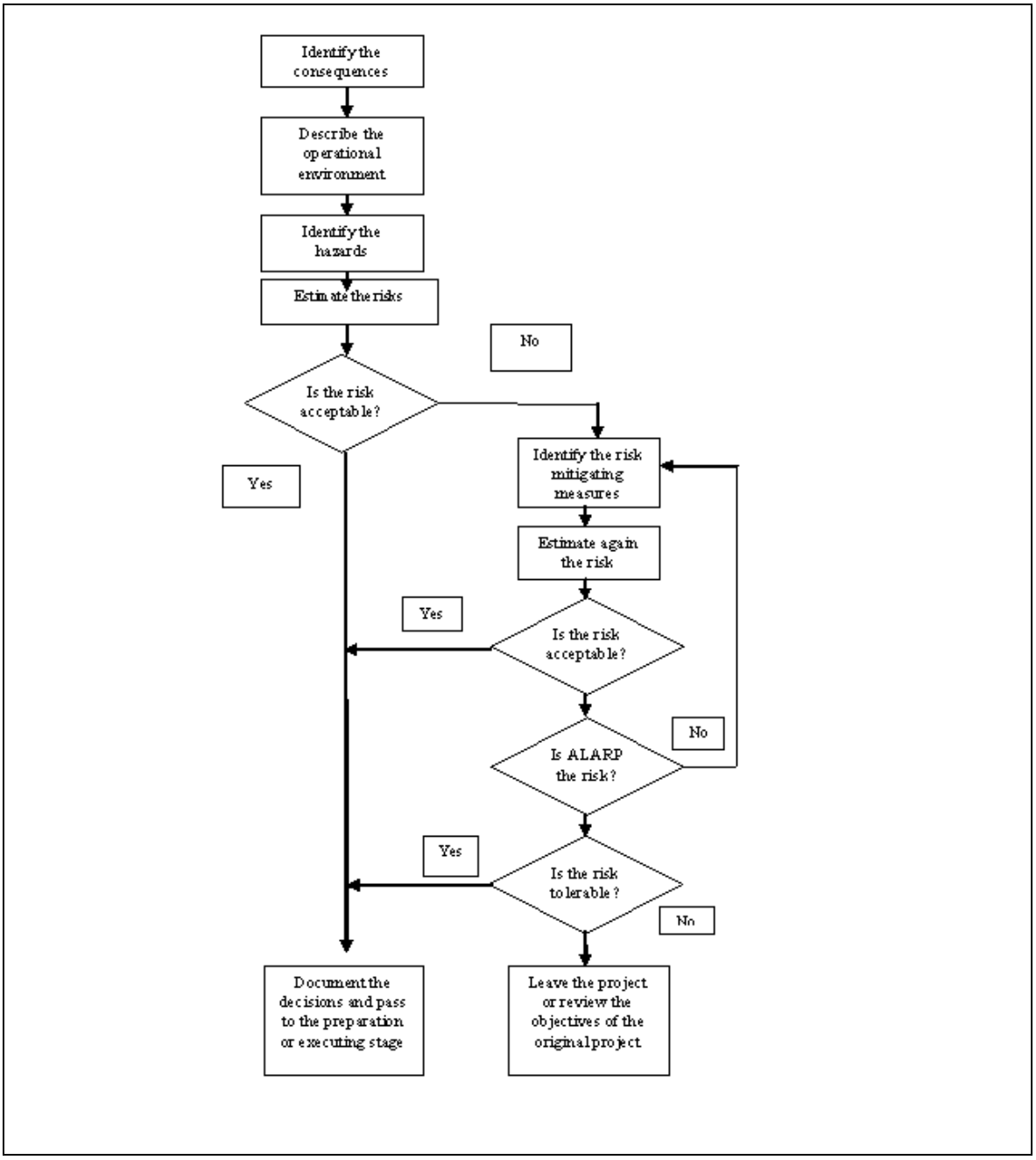


Figure 01 diagram that illustrates safety assessment process

3. Following each of the seven steps of a safety assessment will be examined more thoroughly.

FIRST STEP: FULL DESCRIPTION PREPARATION ON THE SYSTEM TO BE ASSESSED AND THE ENVIRONMENT IN WHICH THE SYSTEM WILL HAVE TO OPERATE

4. The "system" defined for a safety assessment will always be a sub-component of a greater system. For example, even when the assessment comprises all services provided in an aerodrome, it may be considered as a sub-component of a greater regional system, which at the same time is a sub-component of the global aviation system. If all possible hazards must be identified, the persons participating in the safety assessment must have a good comprehension of the new system or the changes proposed and on how will they act in relation to other general system components, of which the new system is part of. In view of this, the First Step of the safety assessment process is to prepare a description of the system or change proposed.

5. The hazard identification process may only identify those hazards comprised within the environment of the system described. Therefore, the system boundaries must be sufficiently wide to cover all possible repercussions that the system may have. In particular, it is important that the description includes the relationships with the major system, of which is part the system subject to assessment.

6. A detailed description of the system should cover the following aspects:

a) Purpose of the system
b) How will the system be used
c) Functions of the system
d) Boundaries and external inter-phases of the system; and
e) Environment in which the system will operate.

7. Repercussions of a possible loss or system degradation in safety shall determine, partially, the characteristics of the operational environment in which the system shall be integrated. Therefore, the description of such environment should include all factors that could have an important effect on safety. These factors shall vary from one case to another; the same could for example include air traffic characteristics, airport infrastructure and factors related with meteorological conditions

8. The system description should also comprise contingency procedures and other non-regular operations, for example, a lack of communications or NAVAIDs. For greater projects, de description of the system should comprise the strategy for the transition of the old system to the new one.

9. For example, will the current system be placed out of service and immediately replaced by the new system, or will both systems operate in parallel for some time?

SECOND STEP: HAZARD IDENTIFICATION

10. At the hazard identification stage, all possible sources of system failure should be studied. Depending on the nature and size of the concerned system, among other, the following sources should be included:

f) Equipment (physical and logical support);
g) Operational environment (i.e. physical conditions, airspace and route design;
h) Human operators;
i) Interphase person-machine;
j) Operational procedures;
k) Maintenance procedures; and
l) External services;
m) Others.

11. All involved parties in the hazard identification process, should be aware of the latent conditions, since they are generally evident. The process should specifically seek for responses to questions such as how could personnel erroneously interpret this procedure? Or how could a person misuse this new function or new system (voluntarily or involuntarily)?

12. The hazard identification stage should be initiated as soon as possible in the project. In great projects, there should be several hazard identification sessions in different stages of the project development. The necessary detail level depends on the complexity of the system considered and the system life cycle moment in which the assessment is carried out. In general, it is expected that less details be necessary for an assessment carried out during the stage of definition of operational requirements that for an assessment carried out during the design stage, which is more thorough.

13. The hazard record should contain a description of each one of the hazards, its consequences, the assessment of its probability and gravity and all required mitigation measure. This record should be updated as new hazards are identified and proposals for its mitigation are presented.

THIRD STEP: ASESSMENT OF THE CONSEQUENCES TO A HAZARD EXPRESSED IN TERMS OF PROBABILITY

14. Within the estimation of probability that a hazard event occurs, a similar approach to the one adopted in the second step must be used; that is to say, through structured discussions, using a standard classification as a guide. **Figure 02** specifies the probability as qualitative categories, but numeric values could also be included, to enable direct numerical estimations on the failure probability. For example, there are often many data available on rates of component failures for several years regarding physical elements of a system.

15. Estimation of the probability that these hazard events occur related generally with human errors, shall suppose a degree of subjective assessment (and it should be kept in mind that even when physical support is assessed, there is always a possibility of human-error failures, such as incorrect maintenance procedures). However, as in the gravity estimation, structured group discussion with participants with a wide experience in their expertise areas, and the adoption of a standardized risk classification, should ensure that the result will be a judgment with full knowledge of the facts.

16. Once the probability assessment for all hazards identified has been completed, the results should be allocated in the hazards record including justification of the classification chosen.

	Meaning	Value
Frequent	Probably will occur several times (has often occurred)	5
Occasional	Probably will occur sometimes (has infrequently occurred)	4
Remote	Improbable but possible to occur (has rarely occurred)	3
Improbable	Very improbable to occur (it is not known if it has occurred)	2
Extremely improbable	Almost unconceivable that the event occurs	1

Figure 02 Probability as qualitative categories

17. Only as information, the following is a quantitative definition in each one of the probabilities of the above figure:

Frequent: 1 a 10^{-3} per flight hour
Occasional: 10^{-3} a 10^{-5} per flight hour
Remote: 10^{-5} a 10^{-7} per flight hour
Improbable: 10^{-7} a 10^{-9} per flight hour
Extremely improbable: $< 10^{-9}$ per flight hour

FOURTH STEP: ASSESSMENT OF THE CONSEQUENCES OF A HAZARD, EXPRESED IN TERMS OF SEVERITY

18. Before initiating this step, the consequences of each hazard identified in the Second and Third Steps should be registered in the record of hazards. The Fourth Step supposes assessment of the severity of each one of these consequences.

19. Risk classification systems have been prepared for a great number of applications in which the hazard analysis is regularly used. An example of one of these systems is shown in the following **Figure 03**:

Gravity of the event	Meaning	Value
Catastrophic	- Equipment destruction - Multiple deaths	A
Dangerous	- Significant reduction in safety margins, physical damage or such a workload that machine operators may not perform their tasks in an accurate and complete manner. - Serious injuries - Major damage to equipment.	B
Major	- Significant reduction of the safety margins, reduction in the ability of the machine operator in responding to adverse operational conditions, as a result of the increment of the workload, or as a result of conditions hindering its efficiency. - Serious incident - Injuries to persons	C
Minor	- Interference - Operational limitations - Use of emergency procedures - Minor incidents	D
Insignificant	- Minor consequences	E

Figure 03 – Severity assessment of events

20. While severity assessment of consequences shall always mean some degree of subjective judgement, structured group discussions, guided by a standardized risk classification and with participants with wide experience in their areas of expertise, should ensure that the result will be a with full knowledge of the facts.

21. Once the gravity assessment of all hazards identified has been completed, the results must be registered in the hazards record, including justification of classification in view of the severity.

FIFTH STEP: RISK RATE/TOLERABILITY

22. Since tolerability or acceptability of a risk depends on its probability and the severity of its consequences, criteria used to judge tolerability will always be bi-dimensional. Therefore, tolerability is generally based in comparison with a severity and probability pattern. **Figure 04** shows and example of pattern for risk tolerability assessment. **Figure 05** shows an example of safety risk tolerability pattern

Risk probability	Risk Severity				
	Catastrophic A	Hazardous B	Major C	Minor D	Negligible E
Frequent 5	5A	5B	5C	5D	5E
Occasional 4	4A	4B	4C	4D	43
Remote 3	3A	3B	3C	3D	3E
Improbable 2	2A	2B	2C	2D	2E
Extremely improbable 1	1A	1B	1C	1D	1E

Figure 04 Pattern for risk tolerability assessment

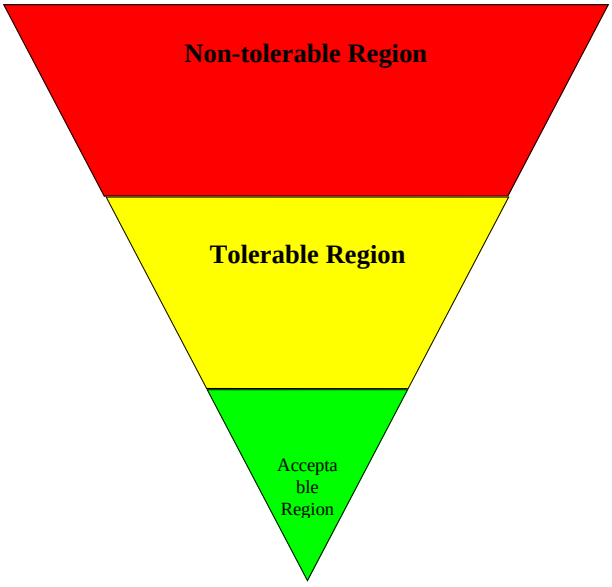
Suggested Criteria	Risk assessment rate	Suggested criteria
	5A, 5B, 5C, 4A, 4B, 3A	Unacceptable under existing circumstances
	5D, 53, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C	Acceptable, based on risk mitigation. May require decision from the directorate
	3E, 2D, 2E, 1A, 1B, 1C, 1D, 1E	Acceptable

Figure 5 Tolerability pattern of safety risk

23. There is an area between the acceptable and inacceptable risk, in which the decision, as regards acceptability is not clear and determinant. These last risks create a third category in which the risk may be tolerable is reduced at the lowest possible level (ALARP). When a risk is classified as ALARP, mitigating measures should be implemented and mitigating measures considered feasible will be applied.

SIXTH STEP: RISK MITIGATION

24. As in the Fifth step, if the risk does not meet predetermined tolerability criteria, it should be intended to reduce it at an acceptable level, or, if not possible, at the lowest practicable level, using appropriate mitigating procedures.

25. The identification of appropriate risk mitigating measures demands a good comprehension of the hazard and the factors that contribute to the occurrence of an event of this type, since all mechanism that is effective to reduce the risk, will have to modify one or more of these factors.

26. Mitigating risk measures may produce an effect reducing the probability that the event or the severity of the consequences, or both, occur. To get to reduce risk at the desired level may demand the application of more than one mitigating measures.

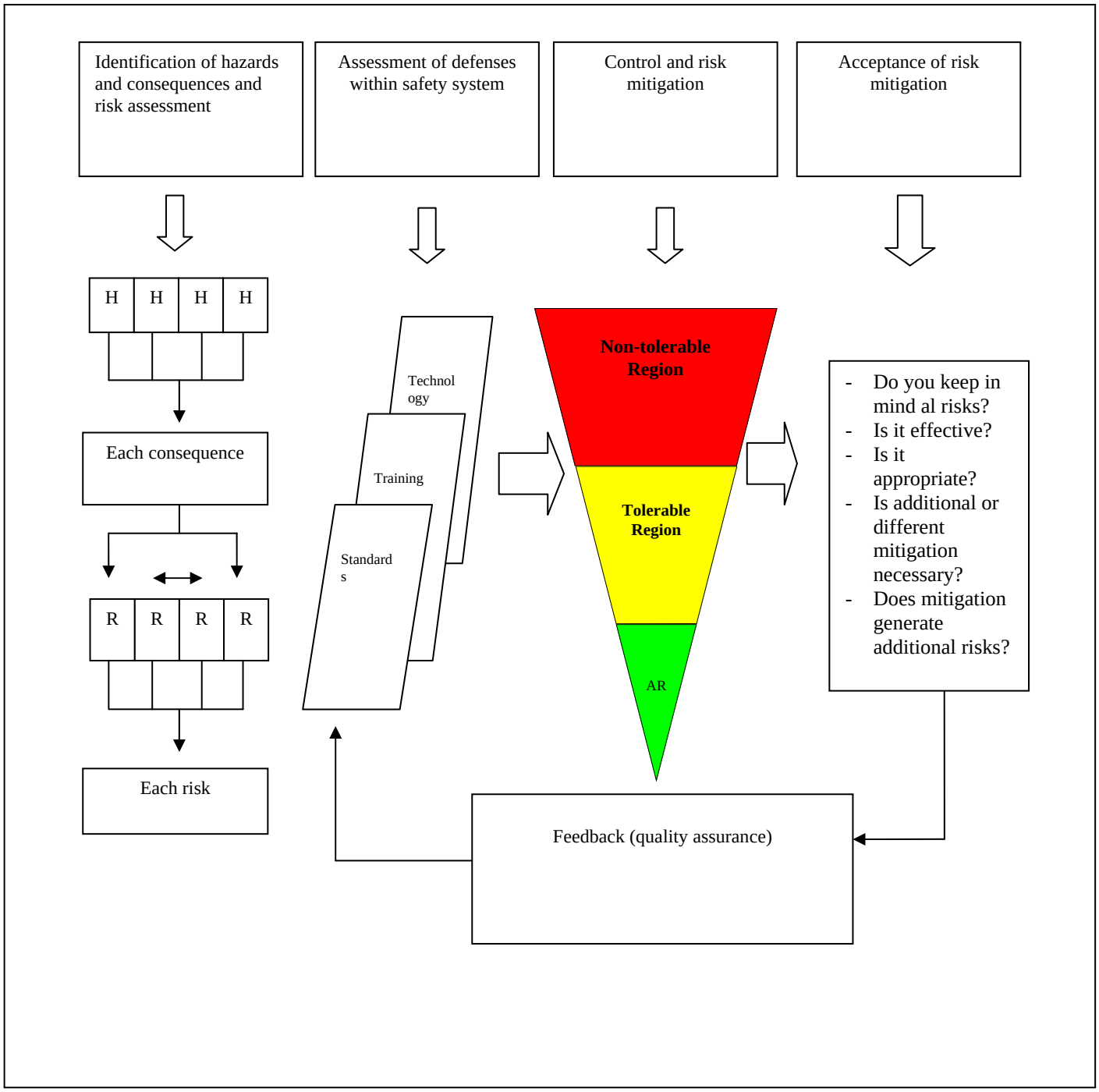
27. Among the possible measures to mitigate risks, the following should be mentioned:

a) Revision of the system design:
b) Changes in operational procedures;
c) Changes in the staff organisation; and
d) Personnel training to face danger.

28. The sooner the hazards in the system life cycle are identified, the easier will it be to change the system design, if required. As the system is closer to its implementation, it will be more difficult and costly to change the design. This could reduce possible mitigating options for those hazards that do are not identified until the last project steps.

29. The effectiveness of all risk mitigating measure proposed must be assessed, first by examining very close if the application of mitigating measures may introduce new hazards, and then repeating Third, Fourth and Fifth steps to assess risk tolerability with the application of proposed mitigating measures.

30. Once the system has been implemented, when results of the supervision are assessed, the safety effectiveness must be thoroughly verified is mitigating measures giving the expected results. **Figure 06** shows the mitigating process of safety risks.


Identification of hazards and consequences and risk assessment
Assessment of defenses within safety system
Control and risk mitigation
Acceptance of risk mitigation
H H H H
Each consequence
R R R R
Each risk
Technol ogy
Training
Standard s
Non-tolerable Region
Tolerable Region
AR
- Do you keep in mind al risks?
- Is it effective?
- Is it appropriate?
- Is additional or different mitigation necessary?
- Does mitigation generate additional risks?
Feedback (quality assurance)

SEVENTH STEP: PREPARATION OF SAFETY ASSESSMENT DOCUMENTS

31. The purpose of safety assessment documents is to have a permanent record of final results of the safety assessment and the arguments and proofs that show that risks related to the system implementation or proposed change have been eliminated or have been adequately controlled and reduced to a tolerable level.

Note.- This presentation of the arguments and proofs to demonstrate safety is mentioned in several safety management texts, as a safety case. Sometimes the expression safety argumentation is sometimes used with a similar meaning.

32. While the safety assessment documents are mentioned here in the last step, during previous steps, a considerable amount of documents will have been produced.

33. In addition to describing the results of a safety assessment, the documentation should have a summary of methods used, hazards identified and mitigating measures necessary to meet safety assessment criteria. The record of hazards should always be included. The documentation should be prepared with sufficient details so that anybody who so wishes, may see not only which decisions were taken, but also which was the justification to classify risks as acceptable or tolerable. It should also include the names of personnel members who participate in the assessment process.

34. The person responsible to carry out a safety assessment and who signs the final acceptance of such assessment will be different, as per the magnitude and complexity of the project and the organization policy. In some cases, it will be the director of the project. When no director of the project has been appointed, it could be the supervisor responsible of the system. In some organizations, the acceptance may require approval of an upper level of administration in case residual risk may not be reduced to an acceptable level, but must be accepted as tolerable and ALARP. The signature of the safety assessment documents by the responsible head, to indicate acceptance, is the final act of the assessment process.