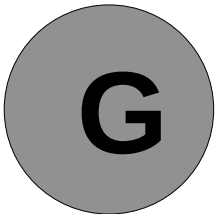


GUIDANCE MATERIAL:

METHODS FOR SETTING SAFETY OBJECTIVES

Safety Objectives (SO) are qualitative or quantitative statements that define the maximum frequency at which a hazard can be accepted to occur.

1 MAKING WORST CREDIBLE CASE ASSUMPTIONS

The purpose of identifying the worst credible case is to specify the relevant level of stringency of Safety Objective: not over stringent (covering some “extreme” cases) and not too lenient (not covering “reasonable” cases).

To be consistent with the 'bias towards safety', assessors should ensure that their assessments make adequate allowance for worst credible case conditions.

It is often difficult to define the boundary between a worst credible case and one so dependent on the co-incidence of unrelated rare events that it should not be taken into account. There is no universally applicable set of rules for setting this boundary, but assessors may find the following guidance helpful in promoting a consistent approach.

A difference should be made between the worst case and the worst credible case.

The worst case identifies the effect that has the most severe consequences. This in many cases could be a Severity 1 (Accident). However, when trying to set a Safety Objective to define, design and operate an ATM system, taking into account this most severe effect could not always lead to set the most stringent safety objective, because the scenario leading to generate this or these Severity 1 effects are so unlikely (many and/or efficient mitigation means or barriers between the hazard and the effect).

In other words, the severity of the hazard effect should not be the only criteria to be taken into account to assess the worst credible case. The risk associated with this scenario leading to generate such an effect should be the criterion and a risk is made of the severity of such effect AND the likelihood of this effect to occur.

The worst credible case aims at identifying the highest contribution of a hazard to a high or the highest risk.

1.1 SAM Definitions

'Worst' means the most unfavourable conditions – e.g. extremely high levels of traffic or extreme weather disruption.

'Credible' implies that it is not unreasonable to expect to experience this combination of extreme conditions within the operational lifetime of the system so that such scenario leading to generate such an effect has to be considered.

Note1: Theses definitions are as per EATMP SAM.

Note2: The word "credible" could lead to difficulties of interpretation, as what is meant is: a combination being "*a believable scenario*" or "*being reasonably pessimistic*". So it obviously includes a subjective part (which should be reduced as much as possible by provision of rationale, field experience data, ..) and requires expert judgement. So other words such as "realistic" or "reasonable" could have been chosen instead of "credible".

However, it was decided to keep this word as it is now being in use for a while.

1.2 Common Cause Analysis (CCA)

Common Cause Analysis is sub-divided into the following areas of study:

- Zonal Safety Analysis (ZSA): should examine each physical zone of the system under assessment to ensure that system installation and potential physical interference with adjacent systems do not violate the independence requirements of the system.

- Particular Risks Assessment (PRA): should examine those common events or influences that are outside the system under assessment but which may violate independence requirements. These particular risks lay also influence several zones at the same time, whereas zonal safety analysis is restricted to each specific zone;

- Common Mode Analysis (CMA): should provide evidence (for the SAM-FHA step) that the failures, failure modes or hazards assumed to be independent are truly independent.

Note: Common Cause Analysis are conducted a certain way during the FHA step of the SAM process to contribute to ensure that the assumptions and results of the FHA (Safety Objectives) are correct. Common Cause Analyses are then to be further continued at the relevant level for the other steps of the SAM (PSSA and SSA).

Note: the level of depth and completeness of the Common Cause Analysis should be commensurate with the stringency of Safety Objectives. So CCA should be extensive and complete for very stringent Safety Objective (for example: if qualitative Safety Objectives are such as “Extremely Rare” or “Rare”) and limited and/or partial for less stringent Safety Objectives (for example: if qualitative Safety Objectives are such as “Occasional ” or “Likely”).

Common Mode Analysis Guidance Material is available in SAE-ARP 4761 (Appendix I: ZSA, J: PRA but to be customised to ANS, K: CMA).

1.3 Consider Flight Phase and Adverse Conditions

Assessors should consider adverse circumstances within the normal range of conditions. The following should be considered:

- The most critical flight phase (failure effects may vary from flight phase to flight phase);

- Adverse environmental and operational conditions (Abnormal or degraded conditions in the system environment could impact the effects of failure occurrence(s), especially if these conditions occur relatively frequently)

1.4 Simultaneous, unrelated failures

In general, assessors need not assume that simultaneous, unrelated external events and failures occur to specify Safety Objectives.

However, assessing scenarii combining simultaneous unrelated failures could be performed to identify additional Safety Requirements bearing either on the Operational Environment or Safety Objectives bearing on the system under assessment when these combinations of unrelated failures are found as being probable.

1.5 What about the other effects?

Many effects may be identified and only one of them is leading to specify the Safety Objective of a specific hazard.

The other effects of a hazard will be also achieving an acceptable risk because they are covered by the worst credible case, as the worst credible case intends to specify the relevant level of stringency of the Safety Objective that make any hazard effect being acceptable risk.

However, sometimes hazards need to be split into many hazards in order to be more precise, for example:

Hazard	Hazard Class (severity of the worst credible hazard effect)
Loss for more than 2’ of [function A] in [Operational environment E]	2

versus

Hazard	Hazard Class (severity of the worst credible hazard effect)
Loss for less than 10” of [function A] in [Operational environment E]	4
Loss for more than 10” and less than 2’ of [function A] in [Operational environment E]	3

Loss for more than 2’ and less than 10’ of [function A] in [Operational environment E]	2
Loss for more than 10’ of [function A] in [Operational environment E]	4

In that case, this has nothing to deal with the worst credible case but with different hazards having different effects and leading to different Safety Objectives and later to different Safety Requirements.

2 QUANTITATIVE METHOD

This method consists of the following steps:

1. Identify all hazard effects.

For each single hazard being identified at the boundary of the system under assessment, all effects of hazard should be identified, taking into account the effectiveness of possible defences (barriers) outside the system under assessment, that could prevent or not the hazard to have certain effect on operations, including the aircraft operations.

2. Allocate severity class to each hazard effect.

After all hazard effects have been identified, severity classification should take place, in accordance with the Severity Classification Scheme. Severity class should be associated with each identified hazard effect.

3. Calculate the conditional probability (Pe).

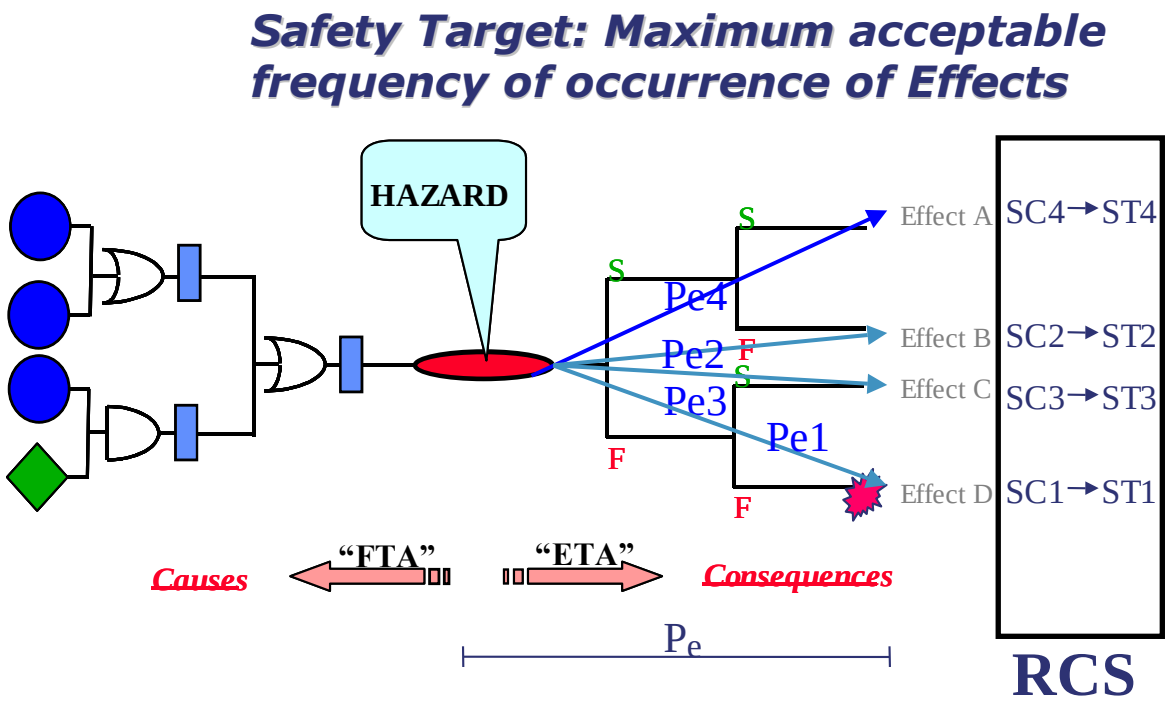
The process of calculating the probability of the hazard to generate each of its effects (Pe) should take place.

4. Allocate the Safety Objective by applying the Risk Classification Scheme.

Risk Classification Scheme/Matrix defined by the Organisation should be used to associate the maximum acceptable rate of occurrence of hazard effect (Safety Target ST)) with the corresponding severity class of the hazard effect.

So, if the overall frequency of hazard effect (ST) is specified in the Risk Classification Scheme provided by the Organisation in terms of maximum

acceptable frequency of occurrence for each severity class, and the probability of the hazard to generate each of its effect is calculated (Pe), than a Safety Objective for the hazard itself is specified by dividing those two values for each different effect and choosing the most stringent one (the lowest figure) between the results,.



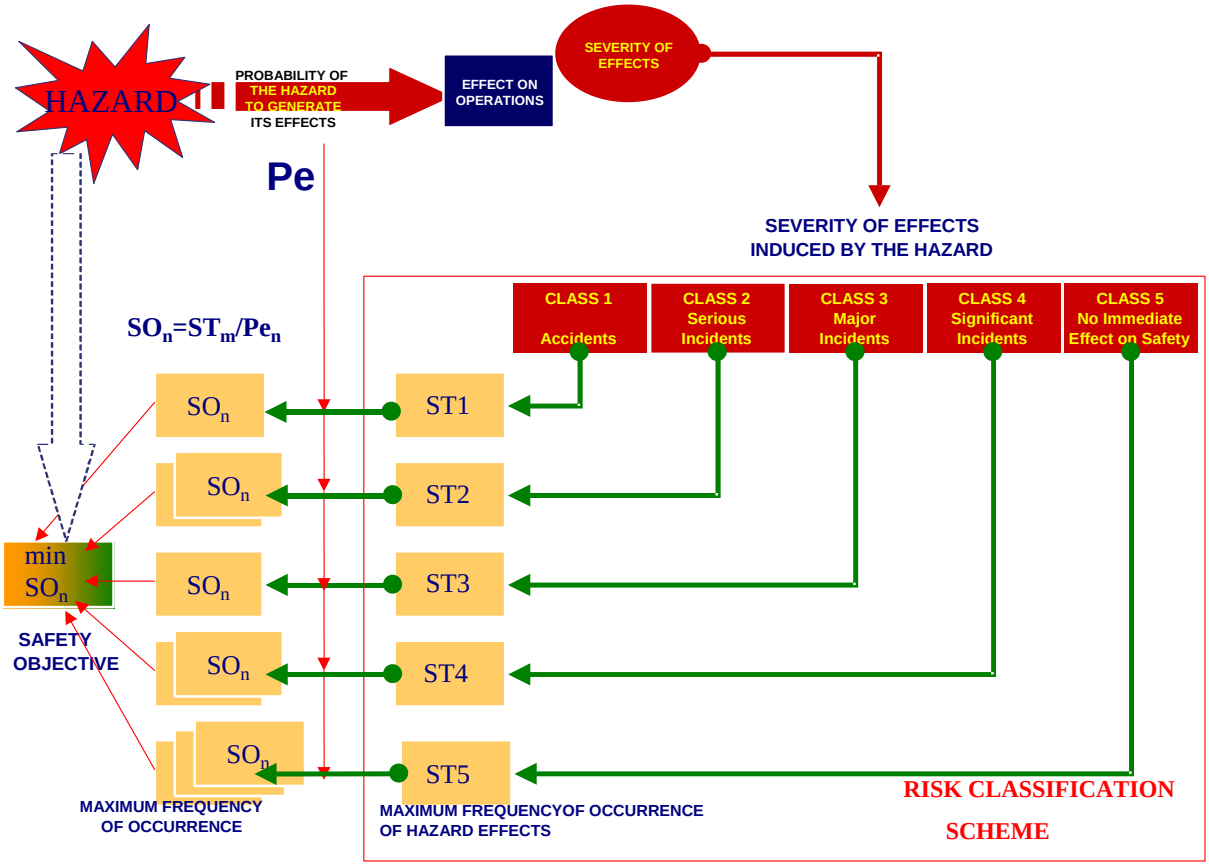
SO = $_{min}$ (ST_m / Pe_n), n = (1,….x) , x = different hazard effects

m = (1,….5) 1, …5 are different severity classes

Note that when applying this method, the principle of the worst credible case is applied when setting the Safety Objective, by choosing the most stringent one, among different values calculated $_{min}$ (ST_m / Pe_n), taking into account not only the severity of the effects but also the probability of the effect as a consequence of the hazard.

Note: the number of hazards is to be taken into account (for example include it in Pe or divide ST_m / Pe_n by the number of hazards for that class of severity) in order to ensure that the sum of all Safety Objectives comply with Safety Targets.

The following figure illustrates the process of setting the Safety Objective using this method.



Advantages of using this method:

1. Fully aligned with the risk definition.

2. Appropriate for the assessment of those systems where the relations between the parts, functions and interfaces are well known, such as hardware, Collision Risk Model, etc.

3. Safety Objectives derived using this method could be less stringent compered with the one derived by using some more conservative method, but the assessment involves a level of details that may provide justification of such less stringent results.

4. Safety Objectives are clear, precise and accurate.

5. It requires very good understanding of contribution of the system being assessed into the overall aviation system.

Limitations of this method:

1. It is not always possible to calculate all the probabilities of hazards generating their effects, so assumptions could be needed in order to quantify them, especially when dealing with barriers relying on human or software.

2. It could be time and effort consuming to calculate all the probabilities.

3. It could be difficult to complete the list of barriers and scenarios that could lead to certain effects.

4. It could require additional effort to transform the units of measurement in order to perform certain calculations.

3 PRESCRIPTIVE METHOD

This method consists of the following steps:

1. Identify all the hazard effects.

For each single hazard being identified at the boundary of the system under assessment, all effects of hazard should be identified, taking into account the effectiveness of possible defences (barriers) outside the system under assessment, that could prevent or not the hazard to generate certain effect on operations, including the aircraft operations.

2. Allocate the severity class to each effect.

After all hazard effects have been identified, severity classification should take place, in accordance with the Severity Classification Scheme. Severity class should be associated with each identified hazard effect.

Note: In fact, this step is not always performed as very often, only step 3 is considered. However, the effectiveness of this method relies on the completeness of the identification of potential effects to make sure that the worst credible case is the correct one.

3. Apply the worst credible case scenario.

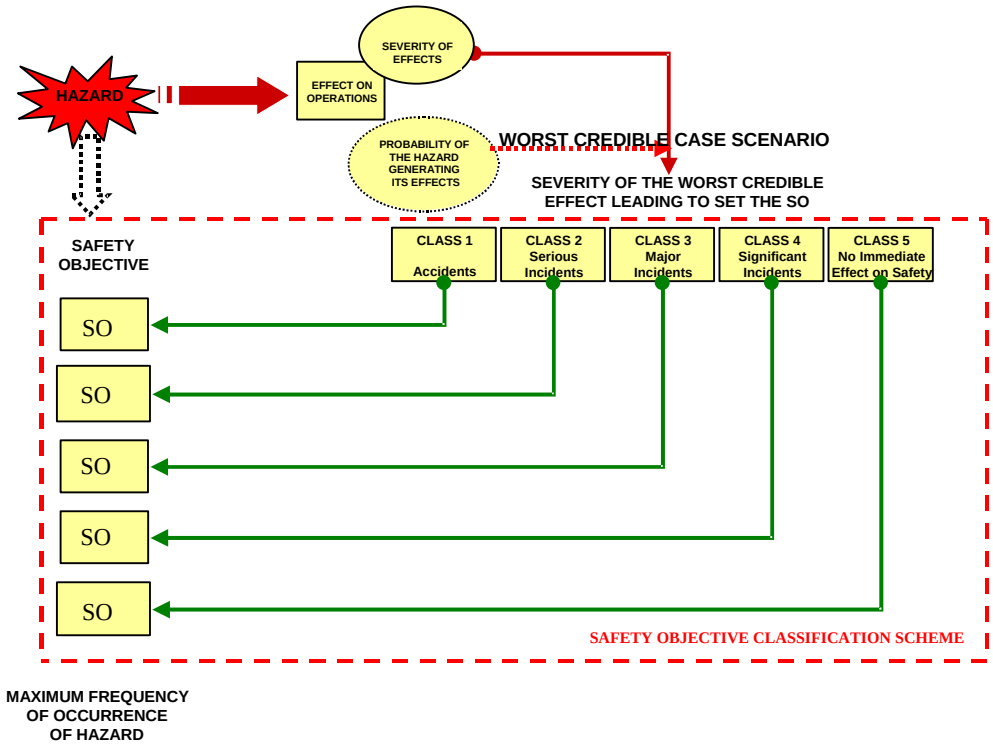
The worst credible effect in the given environment of operation should determine the severity class leading to setting of the Safety Objective,

using expert judgement. It means that somehow the probability of the hazard leading to certain effect (Pe) has been taken into account when deciding the worst credible severity of the hazard effect.

4. Allocate the Safety Objective applying the Safety Objective Classification Scheme.

Safety Objectives are derived directly from the Safety Objective Classification Scheme (See Guidance Material F of this Chapter) that specifies the maximum acceptable frequency of occurrence of a hazard per unit (flight hour, operational hour, per sector, etc) using the severity of its worst credible effect.

The following figure illustrates the process of setting the Safety Objective using this method.



Advantages of this method:

1. It's easier to apply, requires less time, effort and resources, because it doesn't require calculation of the probabilities of the hazard generating the effects (Pe). (It is assumed that they are somehow considered when deciding the severity class that will lead to set the Safety Objective).

2. It ensures harmonisation of the safety assessment process when applied on different system within the same Organisation.

3. It requires less elaboration of the assumptions made for the probabilities of the hazard generating its effects (Pe), since most of them are already embedded in the Safety Objective Classification Scheme.

   (It is assumed that they are included in the Safety Objective Classification Scheme that, as a constant value that applies to all hazards having the severity allocated to their worst credible effect).

Limitations of this method:

1. The appropriateness of the Safety Objective Classification Scheme could lead to over-engineering or under-engineering of the system under assessment: As the same Safety Objective applies to whatever hazard as long as these hazards have the same worst credible effect severity. A Safety Objective Classification Scheme assumes a constant value of the probability of a hazard generating its effect (Pe) for all hazards of the same class (same worst credible effect severity). The answer whether SOCS leads to over or under engineering is known only years after its use being monitored.

2. It can be difficult to demonstrate the link of the SOCS with the organisation Risk Classification Scheme and the Regulatory minimum.

3. It focuses only on the most credibly severe effect of the hazard, without assessing in more details other less severe effects. Any risk has to be mitigated to a acceptable level including those for which the effect has a low level of severity.

4. It doesn't require understanding the contribution of the system under assessment into ATM and overall aviation and the efficiency of the barriers outside the system under assessment (how they can, and more importantly can not, mitigate system hazards).

4 CRITICALITY METHOD

This method consists of the following steps:

1. Identify all the hazard effects.

For each single hazard being identified at the boundary of the system under assessment, all effects of hazard should be identified, taking into account the effectiveness of possible defences (barriers) outside the system under assessment, that could prevent or not the hazard to have certain effect on operations, including the aircraft operations.

2. Allocate the severity class to each effect.

After all hazard effects have been identified, severity classification should take place, in accordance with the Severity Classification Scheme. Severity class should be associated with each identified hazard effect.

3. Estimate the conditional probability (Pe).

The process of estimating the probability of the hazard to generate each of its effects (Pe) should take place.

4. Allocate the Safety Objective by applying Criticality Matrix.

Using the Criticality Matrix and depending on the severity class and the probability of the hazard effect, select the most stringent criticality out of all

Safety Objectives are identified for the hazard in a qualitative terms, as levels of criticality, such as A, B, C or D.

An example of the Criticality Matrix is given below.

Note that all numbers in the example are fictitious.

Example of Criticality Matrix.

Probability of the effect (Pe)	Severity of the Effect				
	1	2	3	4	5
1:1 .. 1:100	A	A or B	B or C	C	D
1:100 .. 1:10.000	A or B	B or C	C	D	D

1:10.000 .. 1:1.000.000	B or C	C	D	D	D
Less than 1:1.000.000	C	D	D	D	D

Levels of Criticality:

A – Very High B – High C – Medium D – Minor

Safety Objectives in terms of Criticality Levels (A, B, C or D) can be transformed in quantitative values, provided that the Organisation has defined its Safety Target (ST). In such case, this method becomes similar to the Quantitative method (see G.1), except that the probabilities of the hazard generating its effects (Pe) are estimated, rather than calculated.

The following figure illustrates the process of setting the Safety Objective using this method.

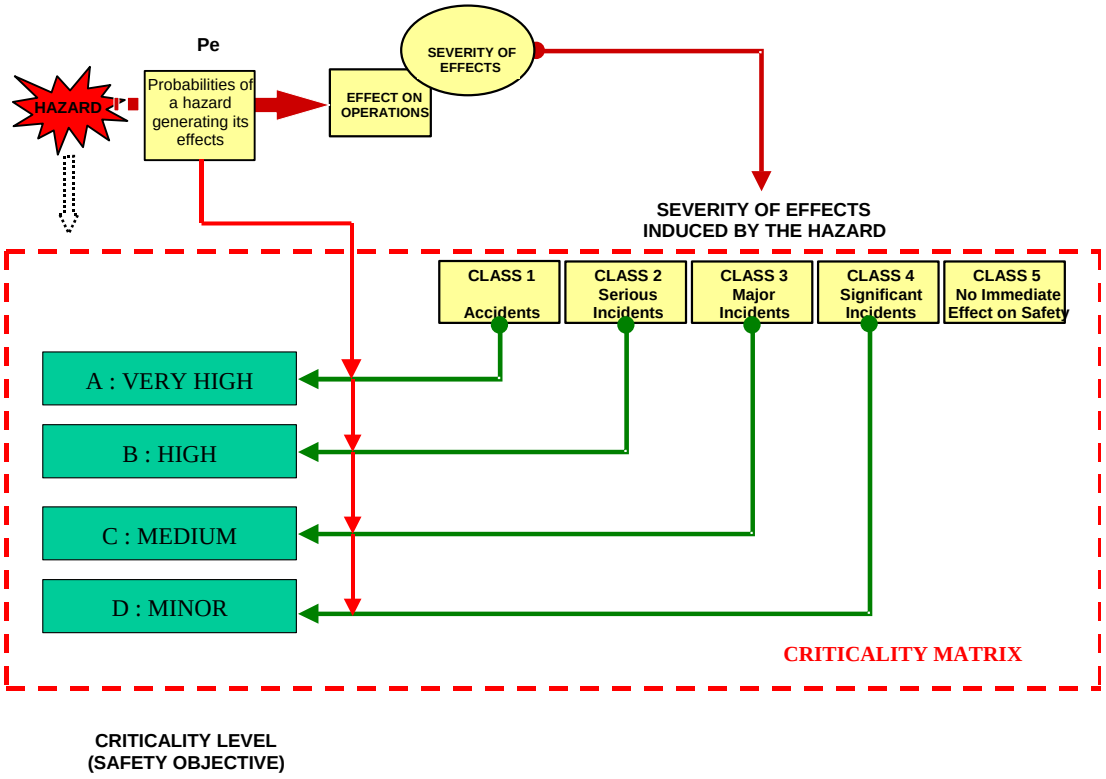


Figure: Safety Objective using Criticality matrix

Advantages of this method:

1. It's more appropriate for assessing systems where precise quantification is difficult due to the nature of the system (software or human elements).

Limitations of this method:

1. This method is more appropriate for identification of Safety Requirements.

2. It requires more elaboration on assumption made on the probabilities of the hazard generating its effects, since they are estimated using expert judgement rather than calculated.

3. If the Safety Objectives expressed in terms of Criticality levels are not related to Safety Target and hence quantified, this method will have the limitations of the Qualitative method.(See G.5)

5 QUALITATIVE METHOD

This method consists of the following steps:

1. Identify all the hazard effects.

For each single hazard being identified at the boundary of the system under assessment, all effects of hazard should be identified, taking into account the effectiveness of possible defences (barriers) outside the system under assessment, that could prevent or not the hazard to generate certain effect on operations, including the aircraft operations.

2. Allocate the severity class to each effect.

After all hazard effects have been identified, severity classification should take place, in accordance with the Severity Classification Scheme. Severity class should be associated with each identified hazard effect.

Note: In fact, this step is not always performed as very often, only step 3 is considered. However, the effectiveness of this method relies on the completeness of the identification of potential effects to make sure that the worst credible case is the correct one.

3. Apply the worst credible case scenario.

The worst credible effect in the given environment of operation should determine the severity class leading to setting of the Safety Objective, using expert judgement. It means that somehow the probability of the hazard leading to certain effect (Pe) has been taken into account when deciding the worst credible severity of the hazard effect.

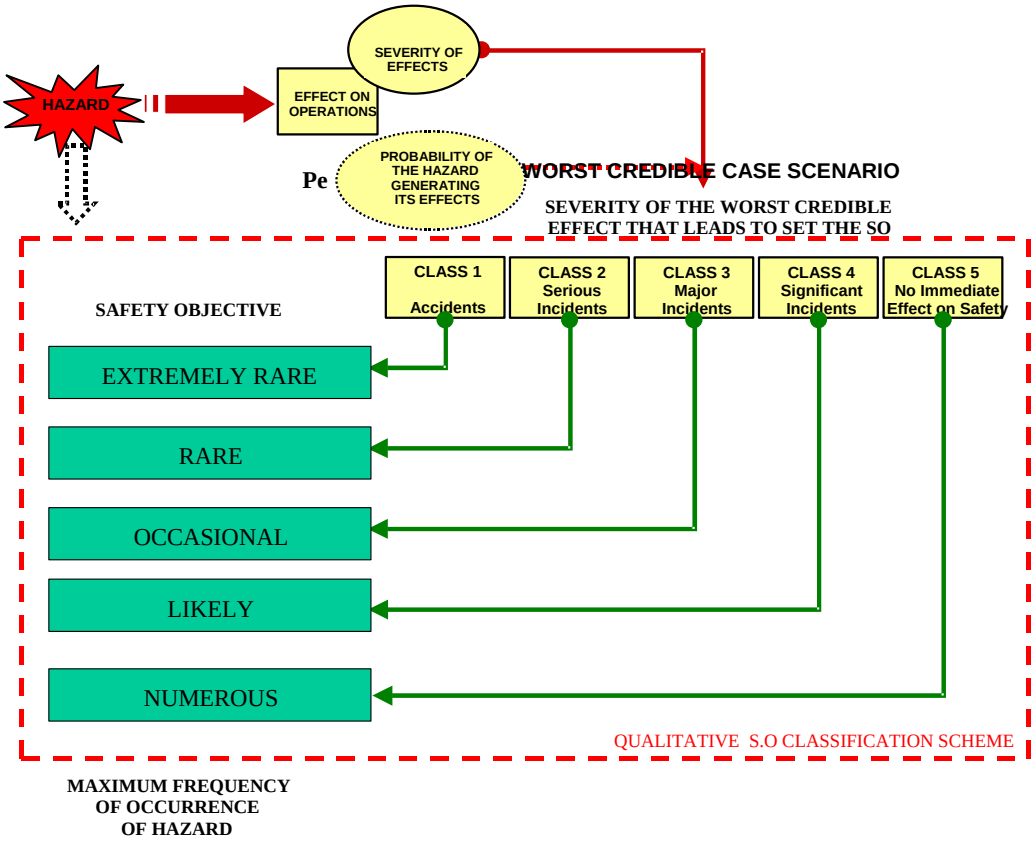
4. Allocate the Safety Objective applying Qualitative Safety Objective Classification Scheme.

Safety Objectives are derived directly from the Organisation Qualitative Safety Objective Classification Scheme which specifies, in qualitative terms, the maximum acceptable frequency of occurrence of a hazard using the severity of its worst credible effect.

An example of a Qualitative Safety Objective Classification Scheme is given below.

Severity Class of the Worst Credible hazard effect [as per ESARR4]	Maximum acceptable frequency of hazard occurrence (Safety Objective)
1	EXTREMELY RARE
2	RARE
3	OCCASIONAL
4	LIKELY
5	NUMEROUS

The following figure illustrates the process of setting the Safety Objective using this method.



A definition of these qualitative categories could be:

Numerous: This effect will certainly happen often throughout the system lifetime.

Likely: This effect will certainly happen several times throughout the system lifetime.

Occasional: This effect may happen sometimes throughout the system lifetime.

Rare: it is not expected to have such an effect more than exceptionally and in some specific circumstances throughout the system lifetime.

Extremely Rare: Such an effect is not expected to happen throughout the system lifetime.

Advantages of this method:

1. It is easy to apply.

2. It's more appropriate for assessing systems where quantification is difficult or impracticable due to the nature of the system (software or human elements). In particular, it can be used as a first step, while waiting for being able later to quantify Safety Objectives.

3. It can be a useful intermediate step before being able to quantify Safety Objectives.

Limitations of this method:

1. As it may not be compliant with ESARR 4, it should be substantiated with the rationale explaining why quantification can not be performed.

2. When it is apportioned into Safety Requirements (especially for equipment), it doesn't provide a clear and unambiguous target for the developers or suppliers of part(s) of the system accustomed to meeting quantified targets. Vendors of such equipment(s) tend to be familiar with quantified specifications, such as reliability/availability/integrity targets.

3. It's not appropriate to show compliance where a quantitative Safety Target has already been specified at the organisation level (for example by the regulator and/or for the whole ANS or ATM organisation or ATC Centre).

4. It doesn't ensure that the net effect on safety is positive in cases where it is expected that some factors of a new system may be allowed to increase the risk, in return for decreases elsewhere, and it is desired to apportion the balance of benefits and disbenefits between the functions at this stage.

6 SAFETY OBJECTIVES SPECIFICATION

For each individual identified hazard, the Safety Objective specifies the maximum acceptable frequency of its occurrence.

Safety Objectives should be specified that way:

> The frequency of [Hazard_Desc] in [Operational_Environment_Desc] shall be no greater than [Value].

The [Value] should be expressed accordingly to the scheme that has been chosen (see §G.2 to G.5 of this chapter)

Safety Objectives should be uniquely identified (SO-ACL-X) and traceable to hazard.

Some examples are given below.

- The frequency of delivering a corrupted, but credible, ATC clearance in the airspace under control by [RST] ATSU shall be no greater than 10^{-6} per clearance.
- The frequency of sending a mis-directed clearance message to one or more aircraft in the airspace under control by [DEF] ATSU shall be no greater than at least an order of magnitude better than that for voice communication.
- The frequency of a spurious alert at any Control Working Position in [ABC] ACC shall be no greater than once in a hundred operating hours.
- The frequency of a total loss of radar separation function for more than 1 minute in [XYZ] TMA sector shall be Extremely Rare.
- The frequency of losing flight level information for more than 10 seconds in sector [ZTV] shall be no greater than Occasional.

7 USE OF HISTORIC DATA

To define quantitative Safety Objectives, historic incident/accident data are often used to establish how much risk a particular system has faced in the past. Care is necessary when using historic data, for the following reasons:

- The more specific the system, the smaller will be the available dataset of incidents and accidents. The number of incidents and accidents specifically relevant to some systems may be too small to be relied upon. Users should take care to ensure an optimum balance between the relevance of the data and their statistical validity.

- Most incidents and accidents have more than one cause. In general, it is only for major accidents that causes are analysed and reported in detail. Hence it is notoriously difficult to apportion incident/accident causes to particular systems. The figures will also depend on whether one considers only primary causes or contributory factors as well.

Basing Safety Objectives on historic data is often the only practicable course, but users should be aware that it does not encourage optimisation of resources. High-risk parts of the operation may be allowed to continue using up a large fraction of the risk budget, when they could perhaps be made safer at reasonable cost. Conversely, expensive resources may continue to be devoted to controlling risks that are relatively small in reality. The iterative refinement of the FHA in later stages of system development should include positive consideration of where risk can most effectively be minimised.