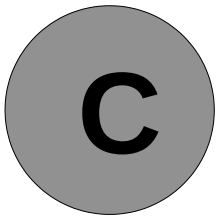


GUIDANCE MATERIAL:

SENSITIVITY ANALYSIS

1 FOREWORD

This paper aims at providing guidance for applying sensitivity analysis technique as part of the Preliminary System Safety Assessment (PSSA).

The purpose of this sensitivity analysis guidance material is not to focus on Safety Requirement quantification, but more to:

- enforce a thorough qualitative analysis of the system design weaknesses leading to identify complementary Safety requirements;
- challenge Safety Requirement credibility;
- assess the impact of divergence from nominal Safety Requirement specification;

- and the identification of possible alternative solutions to balance Safety Requirements.

This Guidance Material is illustrated with an example extracted from a Preliminary System Safety Assessment (PSSA) performed in the framework of the MFF (Mediterranean Free Flight) Project for the ASAS Spacing application “Merge behind”.

PSSA aims at apportioning Safety Objectives into Safety Requirements to the main system elements as follows: aircraft system, ATSP provisions (ground ATC system, controllers), aircraft operator’s provisions (flight crew).

The Safety Requirements allocation process was based on the construction of Fault Trees for a selection of hazards to which quantitative Safety Objectives had been previously allocated and was driven by a sensitivity analysis performed on those fault trees.

The process involved both safety analysis done by engineers and validation of safety results and definition & justification of Safety Requirements in the framework of a workshop held with both operational experts (pilots, controllers) and technical experts (addressing airborne and ground systems supporting the ASAS applications).

2 WHEN TO PERFORM SUCH ANALYSIS

The sensitivity analysis is recommended to be conducted after the Top-Down apportionment of Safety Objectives into Safety requirements (PSSA-SRS Chapter 3 §3.4) was performed.

Such Top-Down apportionment phase is iteratively conducted while the system is design evolves, especially for an end-to-end system design when decisions have to be made to allocate certain Safety Requirements to a part of the end-to-end system (e.g. more on the aircraft equipment or on the pilot or on the ATCO or on the ground ATM equipment or on the Communication segment).

A sensitivity analysis can also be conducted at this level to identify the elements of the system design whose ability to satisfy their Safety Requirements influences greatly the Safety Objective satisfaction (PSSA-SRS Chapter 3 §3.5).

However, sometimes such Top-Down Safety Requirements specification proves difficult to apply down to the lowest architecture element due to lack of data to assess the credibility of certain apportionment or due to modification of an existing design (and not a totally new design).

Therefore, the recommended Top-Down approach can be complemented and completed by the approach described hereafter.

However, it is not recommended to directly start by applying such Bottom-Up approach without performing a Top-Down apportionment as the latter enforces a decision making process of preferred risk mitigation strategies.

3 DESCRIPTION OF THE PROCESS

Two ways of using this process exist:

1. Only steps 4 to 6 apply when the "top-down" apportionment of Safety Objectives into Safety Requirements was performed as recommended in PSSA-SRS Chapter 3 §3.4;

2. Steps 1 to 6 apply when such "top-down" apportionment of Safety Objectives into Safety Requirements was NOT performed as recommended in PSSA-SRS Chapter 3 §3.4.

   Steps 2 & 3 of the process consist in a quantitative bottom-up allocation of probabilities combined with sensitivity analysis (steps 4 & 5) and with an expert validation driven by the sensitivity analysis results (step 6).

Note: This method requires using probability of basic event occurrence. Therefore, a conversion of frequency of occurrence of basic event into probability or a conversion from a unit to another unit (e.g. from /fh to /h) has to be performed. Such conversion requires conversion assumptions that will have to be further verified, validated and monitored.

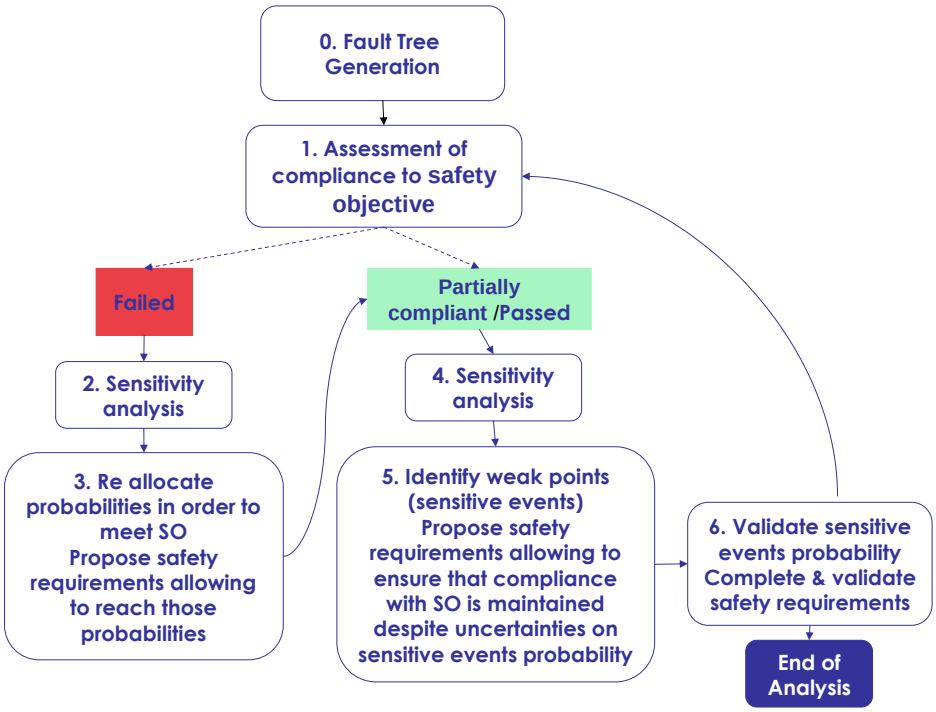
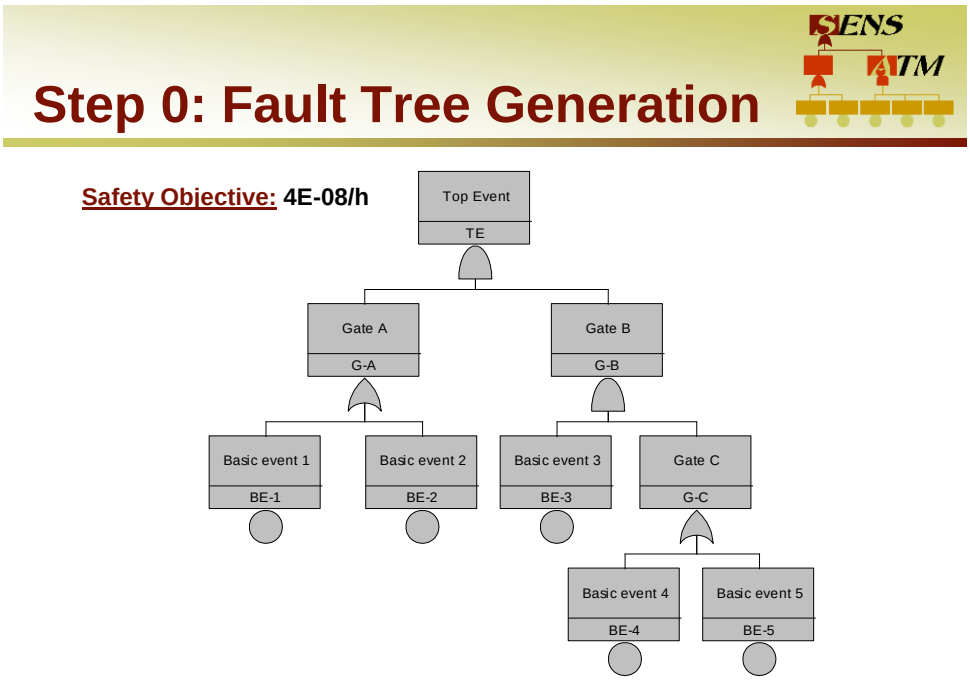


Figure 1 Safety Requirements allocation/balancing driven by sensitivity analysis

The process is iterative and its major steps are shown in Figure 1.

Step 0. Fault-Tree generation

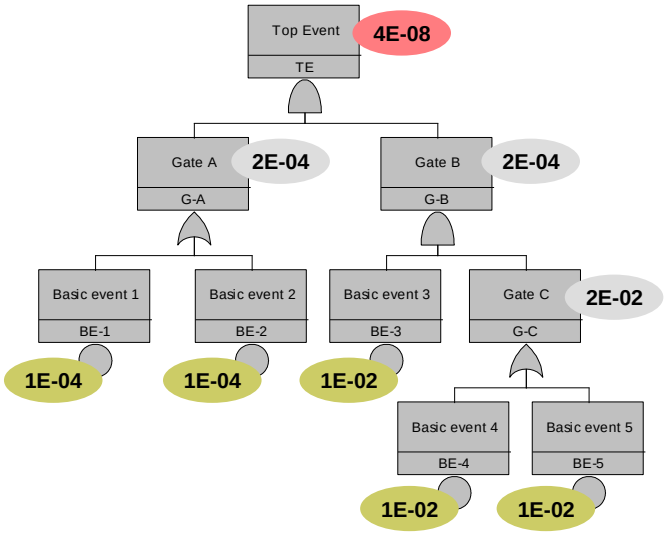
A Fault-Tree has to be created (See SAM-Part IV annex K)



Step 1. Assessment of compliance with Safety Objective (SO):

An initial probability is assigned to each basic event based on engineering judgement (achievable value). Then the probability of occurrence of the top event (operational hazard) is computed and compared with the quantitative Safety Objective (SO) assigned to that hazard.

Step 1: Probabilities assignment



Initial Basic Causes probabilities

SO achieved?	**yes**
Result on Top Event	**4.E-08**
Safety Objective	**4.E-08**

BC#	Basic Cause	Initial Value S1
BE-1	Basic event 1	1.00E-04
BE-2	Basic event 2	1.00E-04
BE-3	Basic event 3	1.00E-02
BE-4	Basic event 4	1.00E-02
BE-5	Basic event 5	1.00E-02

Step 2. Sensitivity analysis (aimed at re-allocation):

In case the top event result does not meet the SO, a sensitivity computation is launched to determine which causes (basic events) probability shall be modified (further decreased) to obtain the required Safety Objective.

Sensitivity analysis allows identification of causes which probabilities variation significantly impacts the resulting top event probability.

Sensitivity analysis is systematically performed on all basic events of the fault tree using certain fault tree dedicated software tools (e.g. ARALIA-SIMTREE or Fault-Tree+[1]).

It consists in multiplying and dividing a basic event probability by some factors (e.g. divided by 100, then10, multiplied by 10, then 100), only one event at a time, in order to assess the potential impact of its variation on the resulting top event probability.

Sensitivity results

SO	4.E-08

BE#	Values S2	(*)0.001	(*)0.01	(*)0.1	(*)1	(*)10	(*)100	(*)1000	Sen
BE-1	1.00E-02	2.19E-08	3.98E-08	2.19E-07	2.02E-06	1.99E-05	1.99E-04	1.99E-04	D100
BE-2	1.00E-04	1.99E-06	1.99E-06	1.99E-06	2.02E-06	2.19E-06	3.96E-06	2.17E-05	N
BE-3	1.00E-02	2.01E-08	2.01E-08	2.01E-07	2.02E-06	2.01E-05	2.01E-04	2.01E-04	D100
BE-4	1.00E-02	1.01E-06	1.02E-06	1.11E-06	2.02E-06	1.10E-05	1.01E-04	1.01E-04	N
BE-5	1.00E-02	1.01E-06	1.02E-06	1.11E-06	2.02E-06	1.10E-05	1.01E-04	1.01E-04	N

[1] EUROCONTROL has sponsored the inclusion of sensitivity analysis function in Fault-Tree+ since V11.

Step 3. Re allocate probabilities in order to meet SO and propose Safety Requirements allowing reaching those probabilities:

A Safety Requirement shall be proposed to ensure that satisfaction of the Safety Objective will be obtained and maintained with the new probabilities.

Safety Requirements take the following content:

- If intent is to mitigate human errors, then qualitative requirement is derived: it could be either a new procedure or the modification of an existing one, or the need to highlight during training the safety importance of a procedure (for example the read-back). Requirement that a specific human action be supported by specific features of a tool may be addressed as well.

- If intent is to mitigate equipment failures, then quantitative requirement is derived: in case of new systems failures, the safety requirement provides the maximal allowable probability of failure. In case of already-operated systems (e.g. failures affecting radar system), requirement stresses need to find out feedback field experience on these particular events in order to compare them with the ones considered as achievable, used as input in the allocation process.

Re-allocated BE probabilities

SO achieved?	no
Result on Top Event	2.01E-06
Safety Objective	4.E-08

BE#	BE	Old Value S2
BE-1	Basic event 1	1.00E-02
BE-2	Basic event 2	1.00E-04
BE-3	Basic event 3	1.00E-02
BE-4	Basic event 4	1.00E-02
BE-5	Basic event 5	1.00E-02

Step 4. Sensitivity analysis (aimed at weak point identification):

When the Safety Objective is met by the top event we have still to ensure that the latter probability will not change significantly through the variation of basic events probabilities (due to uncertainty related to those probabilities). A sensitivity analysis is performed for that effect to highlight the criticality of specific basic events which are identified as “weak points” of the system.

The column “Sensitivity conclusions” (when basic event probability is multiplied &divided by 10/100) the results of that sensitivity analysis are shown as follows:

- M100&D100 indicates that top event result is sensitive to the multiplication/division of that basic event probability by 2 orders of magnitude,
- M10&D10 indicates that result is sensitive to both the multiplication/division of that basic event probability by one order of magnitude.

SO	4.E-08

BE#	Values S2	(*)0.001	(*)0.01	(*)0.1	(*)1	(*)10	(*)100	(*)1000	Sen	(*)0.001	(*)0.01	(*)0.1	(*)10	(*)100	(*)1000
BE-1	1.00E-02	2.19E-10	3.98E-10	2.19E-09	2.01E-08	1.99E-07	1.99E-06	1.99E-06	M10	98.9%	98.0%	89.1%	981.1%	9802.0%	9802.0%
BE-2	1.00E-04	1.99E-08	1.99E-80	1.99E-08	2.01E-08	2.19E-08	3.96E-08	2.17E-07	N	1.0%	1.0%	0.9%	8.8%	97.0%	979.3%
BE-3	1.00E-04	2.01E-11	2.01E-10	2.01E-09	2.01E-08	2.01E-07	2.01E-06	2.01E-05	M10	99.9%	99.0%	90.0%	900.0%	9900.0%	9900.0%
BE-4	1.00E-02	1.01E-08	1.02E-08	1.11E-08	2.01E-08	1.10E-07	1.01E-06	1.01E-06	M10	49.7%	49.3%	44.8%	447.7%	4925.1%	4925.1%
BE-5	1.00E-02	1.01E-08	1.02E-08	1.11E-08	2.01E-08	1.10E-07	1.01E-06	1.01E-06	M10	49.7%	49.3%	44.8%	447.7%	4925.1%	4925.1%

Step 5. Identify weak points (sensitive events) and propose Safety Requirements to ensure that compliance with SO is maintained:

Finally, once sensitive basic events (weak points) have been identified, safety requirements shall be proposed for the system elements displaying these failures, to ensure that despite the uncertainty affecting their probability, the Safety Objective will be satisfied. The advantage of this technique is to target the allocation of Safety Requirements on the weak points (failures with significant contribution to hazards associated to the Safety Objectives).

SR on weak points

BC#	BC	Initial Value	Final Value	SENS	SR#	Safety Requirements
BE-1	**Basic event 1**	**1.00E-04**	**1.00E-02**	**M10**	**SR2**	**Safety Requirements to ensure Safety Objective compliance despite uncertainties on this weak point**
BE-2	Basic event 2	1.00E-04	1.00E-04	N		*Safety requirement no necessary because even if probability assigned is multiplied by 100, the Safety Objective is achieved.*
BE-3	Basic event 3	1.00E-02	1.00E-04	M10	SR1	Safety Requirements to ensure that compliance with the Safety Objective will be obtained and maintained
BE-4	**Basic event 4**	**1.00E-02**	**1.00E-02**	**M10**	**SR3**	**Safety Requirements to ensure Safety Objective compliance despite uncertainties on this weak point**
BE-5	**Basic event 5**	**1.00E-02**	**1.00E-02**	**M10**	**SR4**	**Safety Requirements to ensure Safety Objective compliance despite uncertainties on this weak point**

Step 6. Validate sensitive events probability and complete & validated Safety Requirements:

A validation workshop involving operational (pilots, controllers) and technical experts is needed in order to validate the outcomes of the safety requirements allocation process. The following aspects are addressed:

- Credibility of the sensitive causes and validity of the achievable probability assumed for them (for the human factor related events, a qualitative ranking is used, from the most probable to the less probable one, addressing separately flight crew and controllers; that ranking is further translated in probability orders of magnitude in the next iteration of the allocation process[2]);

  Note that the intent is not to assign an absolute probability value to a human error, bur rather to allow inclusion of the relative contribution of the human errors in the fault trees. The final aim is the sensitivity analysis and not the absolute computation of the human error contribution to the probability of the hazard occurrence

- Safety requirements proposed for each sensitive basic event are validated or invalidated (in terms of credibility, feasibility and effectiveness). When needed and possible, alternative solutions are provided and Safety Requirements are defined in response to those weak points not yet covered by a requirement during the safety analysis allocation steps.

After the workshop the probability values that were modified are re-injected in the fault tree model and the previous steps are re iterated (new sensitivity analysis are performed). In case of major changes (significant changes in the list of sensitive causes), a second validation by experts might be necessary.

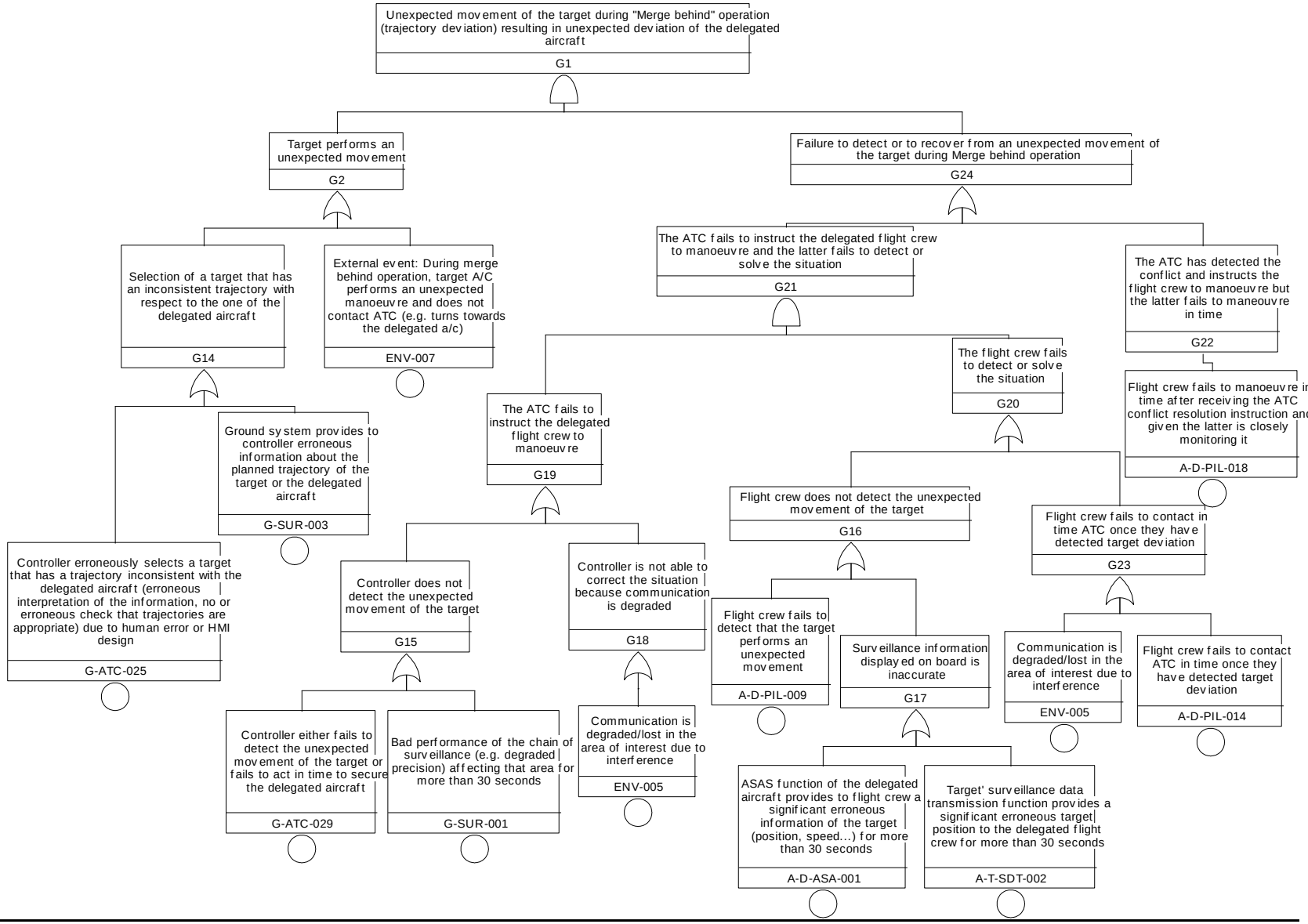
4 EXAMPLE: SENS-ATM APPLIED TO MFF

Step 0: Fault-Tree generation

Figure 2 presents the fault tree that was built for the operational hazard: “Unexpected movement of the target during "Merge behind" operation (trajectory deviation)”.

The Worst Credible effect of this hazard consists in an “unexpected deviation of the delegated aircraft" (Severity Class 2).

The Safety Objective (SO) associated to this hazard is “no more than 1E-07 occurrences per ASAS Spacing operation”.


Unexpected movement of the target during "Merge behind" operation (trajectory deviation) resulting in unexpected deviation of the delegated aircraft
G1
Target performs an unexpected movement
G2
Failure to detect or to recover from an unexpected movement of the target during Merge behind operation
G24
Selection of a target that has an inconsistent trajectory with respect to the one of the delegated aircraft
G14
External event: During merge behind operation, target A/C performs an unexpected manoeuvre and does not contact ATC (e.g. turns towards the delegated a/c)
ENV-007
The ATC fails to instruct the delegated flight crew to manoeuvre and the latter fails to detect or solve the situation
G21
The ATC has detected the conflict and instructs the flight crew to manoeuvre but the latter fails to maneouvre in time
G22
Ground system provides to controller erroneous information about the planned trajectory of the target or the delegated aircraft
G-SUR-003
The ATC fails to instruct the delegated flight crew to manoeuvre
G19
The flight crew fails to detect or solve the situation
G20
Flight crew fails to manoeuvre in time after receiving the ATC conflict resolution instruction and given the latter is closely monitoring it
A-D-PIL-018
Controller erroneously selects a target that has a trajectory inconsistent with the delegated aircraft (erroneous interpretation of the information, no or erroneous check that trajectories are appropriate) due to human error or HMI design
G-ATC-025
Controller does not detect the unexpected movement of the target
G15
Controller is not able to correct the situation because communication is degraded
G18
Flight crew does not detect the unexpected movement of the target
G16
Flight crew fails to contact in time ATC once they have detected target deviation
G23
Flight crew fails to detect that the target performs an unexpected movement
A-D-PIL-009
Surveillance information displayed on board is inaccurate
G17
Communication is degraded/lost in the area of interest due to interference
ENV-005
Flight crew fails to contact ATC in time once they have detected target deviation
A-D-PIL-014
Controller either fails to detect the unexpected movement of the target or fails to act in time to secure the delegated aircraft
G-ATC-029
Bad performance of the chain of surveillance (e.g. degraded precision) affecting that area for more than 30 seconds
G-SUR-001
Communication is degraded/lost in the area of interest due to interference
ENV-005
ASAS function of the delegated aircraft provides to flight crew a significant erroneous information of the target (position, speed…) for more than 30 seconds
A-D-ASA-001
Target' surveillance data transmission function provides a significant erroneous target position to the delegated flight crew for more than 30 seconds
A-T-SDT-002

Step 1. Assessment of compliance with Safety Objective (SO):

The following table provides the list of Safety Requirements allocated using a bottom-up approach for each basic event:

	SO achieved?	**NO**
	Top event (hazard) value	**1E-06**
	Safety Objective (SO)	**1E-07**
Event Label	**Event Description**	**Basic Event achievable probability**
A-D-ASA-001	ASAS function of the delegated aircraft provides to flight crew a significant erroneous information of the target (position, speed,,,) for more than 30 seconds	1E-06
A-D-PIL-009	Flight crew fails to detect that the target performs an unexpected movement	0.01
A-D-PIL-014	Flight crew fails to contact ATC in time once they have detected target deviation	1E-05
A-D-PIL-018	Flight crew fails to manoeuvre in time after receiving the ATC conflict resolution instruction and given the latter is closely monitoring it	0,001
A-T-SDT-002	Target' surveillance data transmission function provides a significant erroneous target position to the delegated flight crew for more than 30 seconds	1E-05
ENV-005	Communication is degraded/lost in the area of interest due to interference	1E-05
ENV-007	External event: During merge behind operation, target A/C performs an unexpected manoeuvre and does not contact ATC (e,g, turns towards the delegated a/c)	1E-04
G-ATC-025	Controller erroneously selects a target that has a trajectory inconsistent with the delegated aircraft (erroneous interpretation of information, no or erroneous check that trajectories are appropriate) due to human error or HMI design	0.001
G-ATC-029	Controller either fails to detect the unexpected movement of the target or fails to act in time to secure the delegated aircraft	0.001
G-SUR-001	Bad performance of the chain of surveillance (e,g, degraded precision) affecting that area for more than 30 s	1E-07
G-SUR-003	Ground system provides to controller erroneous information about the planned trajectory of the target or the delegated aircraft	1E-05

Table 1.1: MFF initial Safety Requirements definition

The achievable Safety Objective (Top event value) with such values is 1.13 E-6.

Step 2. Sensitivity analysis (aimed at re-allocation)

Table 2.1 provides the results of the sensitivity analysis aimed at re-allocating probabilities to obtain the required Safety Objective. The basic events A-D-PIL-018 and G-ATC-025 are the most sensitive with respect to a division by 10 of their respective probabilities and modification by that order of either of those events allows to reach the SO (top event probability passes from 1.2E-06 to 2.3E-07 which is judged acceptable[3]).

Evt Label	Evt Description	Basic Evt achievable probability	Top event probability - sensitivity computation				
			(*)0,01	(*)0,1	(*)1	(*)10	(*)100
A-D-ASA-001	ASAS function of the delegated aircraft provides to flight crew a significant erroneous information of the target (position, speed,,,) for more than 30 seconds	1E-06	1.13e-6	1.13e-6	1.13e-6	1.13e-6	1.13e-6
A-D-PIL-009	Flight crew fails to detect that the target performs an unexpected movement	0.01	1.12e-6	1.12e-6	1.13e-6	1.23e-6	2.22e-6
A-D-PIL-014	Flight crew fails to contact ATC in time once they have detected target deviation	1E-05	1.13e-6	1.13e-6	1.13e-6	1.13e-6	1.13e-6
A-D-PIL-018	Flight crew fails to manoeuvre in time after receiving the ATC conflict resolution instruction and given the latter is closely monitoring it	0,001	3.33e-8	**1.33e-7**	1.13e-6	1.11e-5	1.11e-4
A-T-SDT-002	Target' surveillance data transmission function provides a significant erroneous target position to the delegated flight crew for more than 30 seconds	1E-05	1.13e-6	1.13e-6	1.13e-6	1.13e-6	1.13e-6
ENV-005	Communication is degraded/lost in the area of interest due to interference	1E-05	1.12e-6	1.12e-6	1.13e-6	1.23e-6	2.22e-6
ENV-007	External event: During merge behind operation, target A/C performs an unexpected manoeuvre and does not contact ATC (e,g, turns towards the delegated a/c)	1E-04	1.03e-6	1.04e-6	1.13e-6	2.04e-6	1.12e-5
G-ATC-025	Controller erroneously selects a target that has a trajectory inconsistent with the delegated aircraft (erroneous interpretation of information, no or erroneous check that trajectories are appropriate) due to human error or HMI design	0.001	1.22e-7	**2.14e-7**	1.13e-6	1.03e-5	1.02e-4
G-ATC-029	Controller either fails to detect the unexpected movement of the target or fails to act in time to secure the delegated aircraft	0.001	1.12e-6	1.12e-6	1.13e-6	1.23e-6	2.23e-6
G-SUR-001	Bad performance of the chain of surveillance (e,g, degraded precision) affecting that area for more than 30 s	1E-07	1.13e-6	1.13e-6	1.13e-6	1.13e-6	1.13e-6
G-SUR-003	Ground system provides to controller erroneous information about the planned trajectory of the target or the delegated	1E-05	1.12e-6	1.12e-6	1.13e-6	1.22e-6	2.14e-6

[3] To further decrease that value to 1E-07 the probability of G-ATC-025 shall be divided by 2. Nevertheless, given the uncertainty affecting the human errors occurrence, we accept to work with orders of magnitudes and define effective Safety Requirements to mitigate risk associated to those errors.

	aircraft						

Table 2.1. Example of Safety Requirements re-allocation

Step 3. Re-allocate probabilities in order to meet Safety Objectives and propose Safety Requirements allowing reaching those probabilities:

In the chosen example, both basic events A-D-PIL-018 and G-ATC-025 are candidates to be re-allocated a value of 1E-04 instead of the current 1E-03, but only one change would be enough.

Changing A-D-PIL-018 is chosen, given that a credible and effective Safety Requirement was found (see line corresponding to A-D-PIL-018 in Table 2.1).

Step 4. Sensitivity analysis (aimed at weak points identification):

As a result of the sensitivity analysis performed after the previous re-allocation, the events A-D-PIL-009, G-ATC-029 and ENV-005, ENV-007 were found sensitive as the multiplication by 10 of the former two and by 100 of the latter two involves a significant increase (one order of magnitude) of the top event probability (note that an updated table 1.1, not included here, is obtained).

Evt Label	Evt Description	Basic Evt achievable probability	Top event probability - sensitivity computation				
			(*)0,01	(*)0,1	(*)1	(*)10	(*)100
A-D-ASA-001	ASAS function of the delegated aircraft provides to flight crew a significant erroneous information of the target (position, speed,,,) for more than 30 seconds	1E-06	1.13e-6	1.13e-6	1.13e-6	1.13e-6	1.13e-6
A-D-PIL-009	Flight crew fails to detect that the target performs an unexpected movement	0.01	1.12e-6	1.12e-6	1.13e-6	1.23e-6	**2.22e-6**
A-D-PIL-014	Flight crew fails to contact ATC in time once they have detected target deviation	1E-05	1.13e-6	1.13e-6	1.13e-6	1.13e-6	1.13e-6
A-D-PIL-018	Flight crew fails to manoeuvre in time after receiving the ATC conflict resolution instruction and given the latter is closely monitoring it	0,001	3.33e-8	1.33e-7	1.13e-6	**1.11e-5**	**1.11e-4**
A-T-SDT-002	Target' surveillance data transmission function provides a significant erroneous target position to the delegated flight crew for more than 30 seconds	1E-05	1.13e-6	1.13e-6	1.13e-6	1.13e-6	1.13e-6
ENV-005	Communication is degraded/lost in the area of interest due to interference	1E-05	1.12e-6	1.12e-6	1.13e-6	1.23e-6	**2.22e-6**
ENV-007	External event: During merge behind operation, target A/C performs an unexpected manoeuvre and does not contact ATC (e,g, turns towards the delegated a/c)	1E-04	1.03e-6	1.04e-6	1.13e-6	**2.04e-6**	**1.12e-5**

Evt Label	Evt Description	Basic Evt achievable probability	Top event probability - sensitivity computation				
			(*)0,01	(*)0,1	(*)1	(*)10	(*)100
G-ATC-025	Controller erroneously selects a target that has a trajectory inconsistent with the delegated aircraft (erroneous interpretation of information, no or erroneous check that trajectories are appropriate) due to human error or HMI design	0.001	1.22e-7	2.14e-7	1.13e-6	**1.03e-5**	**1.02e-4**
G-ATC-029	Controller either fails to detect the unexpected movement of the target or fails to act in time to secure the delegated aircraft	0.001	1.12e-6	1.12e-6	1.13e-6	1.23e-6	**2.23e-6**
G-SUR-001	Bad performance of the chain of surveillance (e,g, degraded precision) affecting that area for more than 30 s	1E-07	1.13e-6	1.13e-6	1.13e-6	1.13e-6	1.13e-6
G-SUR-003	Ground system provides to controller erroneous information about the planned trajectory of the target or the delegated aircraft	1E-05	1.12e-6	1.12e-6	1.13e-6	1.22e-6	**2.14e-6**

Table 4.1: Identification of weak points

Step 5. Identify weak points (sensitive events) and propose Safety Requirements to ensure that compliance with SO is maintained:

According to table 4.1, Safety Requirements were defined for each of the previously identified weak points.

Note that A-D-PIL-009, G-ATC-029 and G-ATC-025 display the highest sensitivity with respect to the increase of their probability and thus the Safety Requirements defined for mitigating them need particular attention when checking their effectiveness. Be aware that in the real process, some of these requirements are proposed at this step, others need to be amended or new ones added during the next step.

Step 6. Validate sensitive events probability and complete & validated Safety Requirements:

In Table 2, the last three columns reflect that iteration.

Note that following the workshop validation, the probability for G-ATC-029 was relaxed from 0.001 to 0.01. In the example neither the allocation nor the list of weak points were called into question following the validation step and the second iteration of sensitivity analysis.

Nevertheless the sensitivity of weak points A-D-PIL-009 and G-ATC-029 with respect to the increase of their probability becomes higher, and thus the Safety Requirements defined for mitigating them need particular attention when checking their effectiveness.

Cause Identifier	Cause (basic event) definition	Achievable probability (→ reallocated when necessary to meet SO)	Sensitivity conclusions after re-allocation (when basic event probability is multiplied &divided by 10/100)	Workshop validated/ allocated probability	Re-Sensitivity conclusions (based on validation outputs)	Validated Safety Requirement
A-D-PIL-009	Flight crew fails to detect that the target performs an unexpected movement	0.01	M100	Same	M10	To provide an appropriate HMI (e.g. visualisation precise enough or function allowing to highlight a significant target deviation) and sufficient training allowing the flight crew to easily/fastly detect an unexpected movement of the target
A-D-PIL-018	Flight crew fails to manoeuvre in time after receiving the ATC conflict resolution instruction and given the latter is closely monitoring it	0.001 → Changed to 1,00E-04 to meet the SO	D&M10	Same	M10	Use of ICAO phraseology that allows the controller to indicate to flight crew the emergency of the manoeuvre performance (e.g. essential traffic) shall be re-enforced for ASAS During the flight crews' training, it shall be highlighted that emergency situations are also applicable to ASAS
ENV-005	External event: Communication is degraded/lost in the area of interest due to interference	1E-05	M100	Same	M100	To be confronted with field feedback experience
ENV-007	External event: During merge behind operation, target A/C performs an unexpected manoeuvre and does not contact ATC (e.g. turns towards the delegated a/c)	1E-04	M100	Same, waiting for confrontation with field feedback experience	M100	In case the field feedback experience probability is of an order of magnitude of 1e-03 per ASAS delegation (or 3e-03 flight/hour) or worse, in areas where ASAS spacing is implemented (stipulated by AIP), the following safety requirement is proposed: "The normal procedure that states that aircraft shall contact controllers if they deviate from current trajectory shall be reinforced".
G-ATC-025	Controller erroneously selects a target that has a trajectory inconsistent with the delegated aircraft (erroneous interpretation of the information, no or erroneous check that trajectories are appropriate) due to human error or HMI design	0.001	D&M10	same	D&M10	A ground system shall be designed to help the controllers in selecting pairs of aircraft for ASAS spacing instruction having appropriate trajectories
G-ATC-029	Controller either fails to detect the unexpected movement of the target or fails to act in time to secure the delegated aircraft	0.001	M100	0.01 after validation workshop	M10	Two complementary requirements are issued: 1. Trajectory Change Points (TCP) shall be downlinked to the ground The controller shall be alerted of inconsistency between a/c trajectory selected on ground and the one selected on FMS. 2; Appropriate means on CWP shall be provided allowing controllers to correctly monitor the spacing (e.g. to provide an alert in case of predicted infringement of ASAS spacing on CWP)

(D = Division by; M = Multiplication by)

Table 6.1: Synthetic results of the allocation process driven by sensitivity analysis