Safety Analysis Methodology for ADS-B Based Surveillance Applications

Jonathan Hammer, The MITRE corporation
Gilles Caligaris, EUROCONTROL
Marta Llobet, EGIS Avia (Sofréavia)

Content

1. ADS-B background and safety
2. Joint US/Europe Safety Assessment Methodology for ADS-B
3. Case Study: ADS-B-NRA Safety Assessment
4. Conclusion

ADS-B Applications & Safety Background

1
2
3
4

Applications

Air-to-Air:
- Parallel runways
- Spacing & Merging
- Air-to-air / Airport Surface Situational Awareness

Air-to-ground:
- Non-Radar Areas
- Radar Areas
- Airport Areas

Package 1:
- A set of ADS-B applications,
- Internationally agreed

Safety

- Internationally agreed frameworks
  - TCAS
  - data link communications services.
  - Techniques not directly applicable to ADS-B applications
- ADS-B safety work done in US and Europe independently
- Need for joint safety effort

RFG: OSEDS, Safety and Performance Requirements (SPR)
FAA, EUROCONTROL, RTCA, EUROCAE, AirServices Australia, Japan

RFG Safety Assessment Methodology

1
2
3
4

- Joint US/Europe
- Focuses on ADS-B applications.
- Applies to surveillance components but also to other CNS/ATM system elements
- Mainly based on:
  - ED78A/DO264
  - EUROCONTROL SAM
  - FAA SMS (Safety Management System) Process
- Aimed at delivering safety requirements for the standard

Main Steps

1
2
3
4

OSED: Operational Services & Environment Definition

Safety Process:

- **OHA**: Operational Hazard Identification and Assessment
- **ASOR**: Allocation of Safety Objectives and Requirements

Performance requirements

Operational requirements

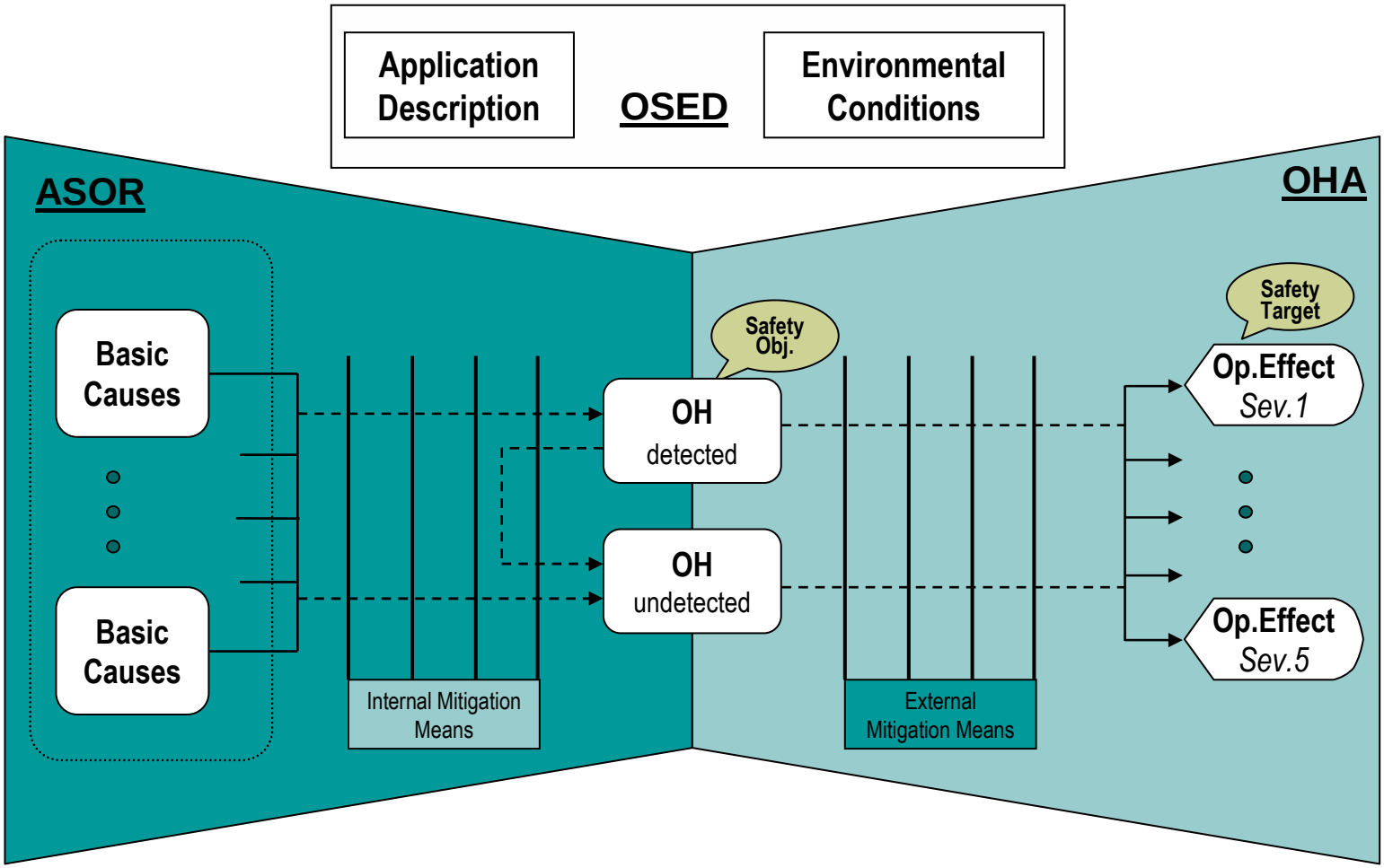
Interoperability requirements

Safety Requirements

SPR
document

1
2
3
4

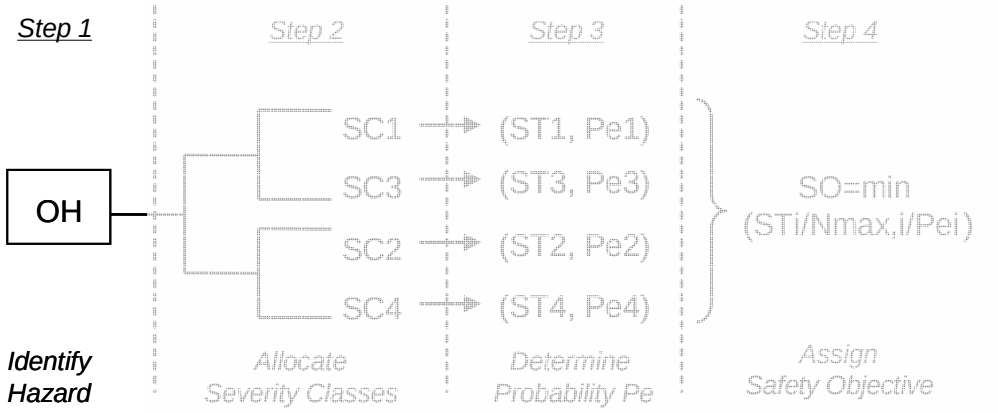
Safety Assessment Overview



1
2
3
4

OHA Process

1. Hazard Identification

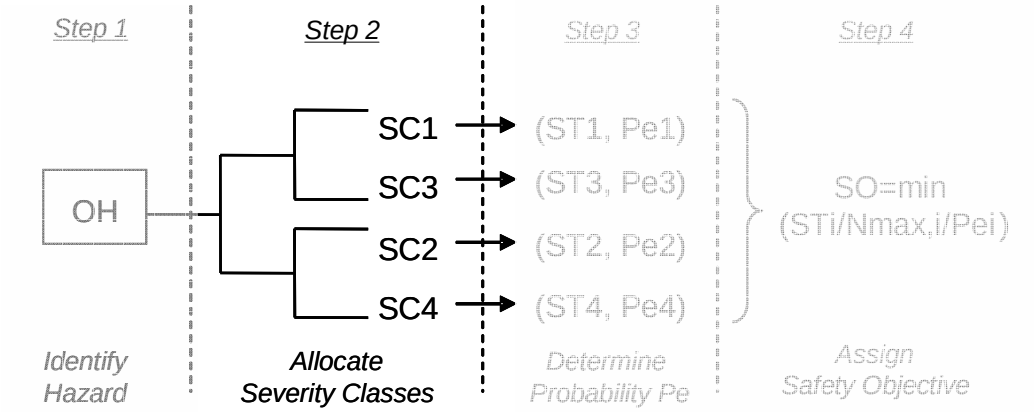


- Brainstorming sessions with operational experts:
  - air-traffic controllers
  - Pilots
  - Safety experts
- Hazards identified between causes and operational effects level.
- Detected and Undetected hazards are identified

1
2
3
4

OHA Process

2. Severity Class Allocation

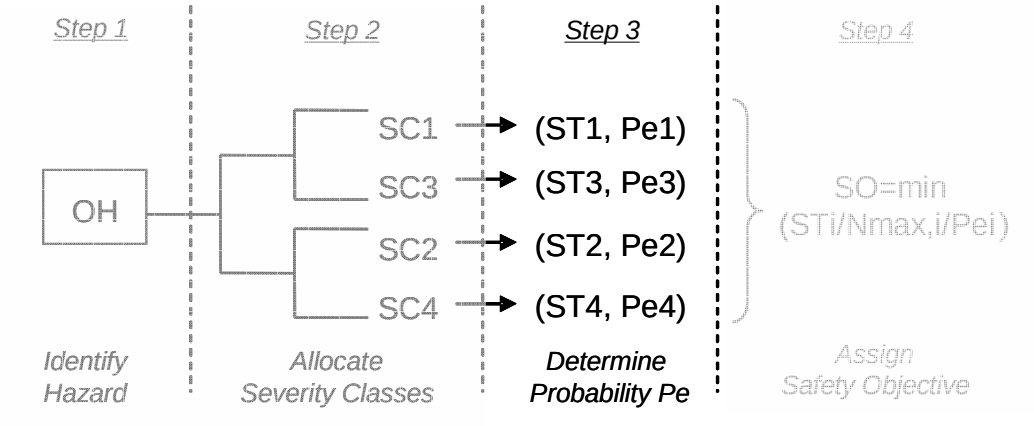


Hazard Class	1 (most severe)	2	3	4	5 (least severe)
Effect on Operations	Normally with hull loss. Total loss of flight control, mid-air collision, flight into terrain or high speed surface movement collision.	Large reduction in safety margins or aircraft functional capabilities.	Significant reduction in safety margins or aircraft functional capabilities.	Slight reduction in safety margins or aircraft functional capabilities.	No effect on operational capabilities or safety
Effect on Occupants	Multiple fatalities.	Serious or fatal injury to a small number of passengers or cabin crew.	Physical distress, possibly including injuries.	Physical discomfort.	Inconvenience.
Effect on Air crew	Fatalities or incapacitation.	Physical distress or excessive workload impairs ability to perform tasks.	Physical discomfort, possibly including injuries or significant increase in workload.	Slight increase in workload.	No effect on flight crew.
Effect on Air Traffic Service	Total loss of separation.	Large reduction in separation or a total loss of air traffic control for a significant period of time.	Significant reduction in separation or significant reduction in air traffic control capability.	Slight reduction in separation or in ATC capability. Significant increase in air traffic controller workload.	Slight increase in air traffic controller workload.
Example of ASAS operational effects	• *Mid-air collision* • *Controlled flight into terrain* • *Total loss of flight control* • *High speed surface movement collision (i.e. collision in runway)* • *Leaving a prepared surface at high speed.*	• *Large reduction in separation or safety margins* • *Loss of separation resulting in wake vortex encounter at low altitude.* • *Large reduction in safety margins like abrupt maneuver is required to avoid mid-air collision or CFIT (e.g. one or more aircraft deviating from their intended clearance)* • *Large reduction in aircraft functional capabilities* • *Total loss of air traffic control for a significant period of time*	• *Significant reduction in separation or safety margins* • *Loss of separation resulting in wake vortex encounter at high altitude.* • *Low speed surface movement collision (i.e. collision in taxiway)* • *Leaving a prepared surface at low speed* • *Significant reduction in aircraft functional capabilities* • *Significant reduction in air traffic control capability*	• *Slight reduction in separation or safety margins* • *Significant increase in air traffic controller workload* • *Slight increase in flight crew workload*	• *No effect on operations /traffic* • *Slight increase in air traffic controller workload* • *No effect on flight crew*

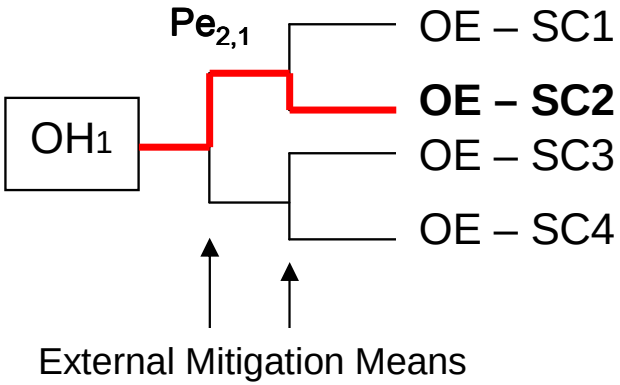
1
2
3
4

OHA Process

3. Determine Probability Pe



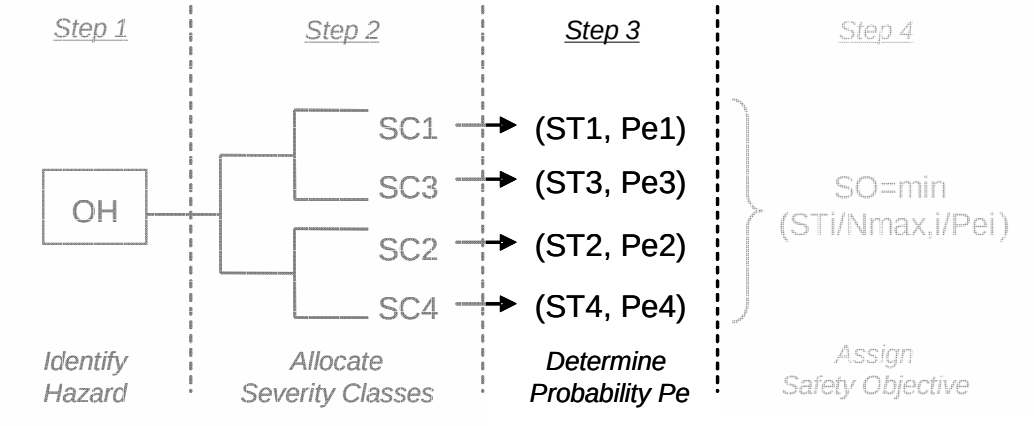
- *Equivalent probability* ***Pe***: conditional probability which expresses the probability that the occurrence of a hazard will results in a specific operational effect.

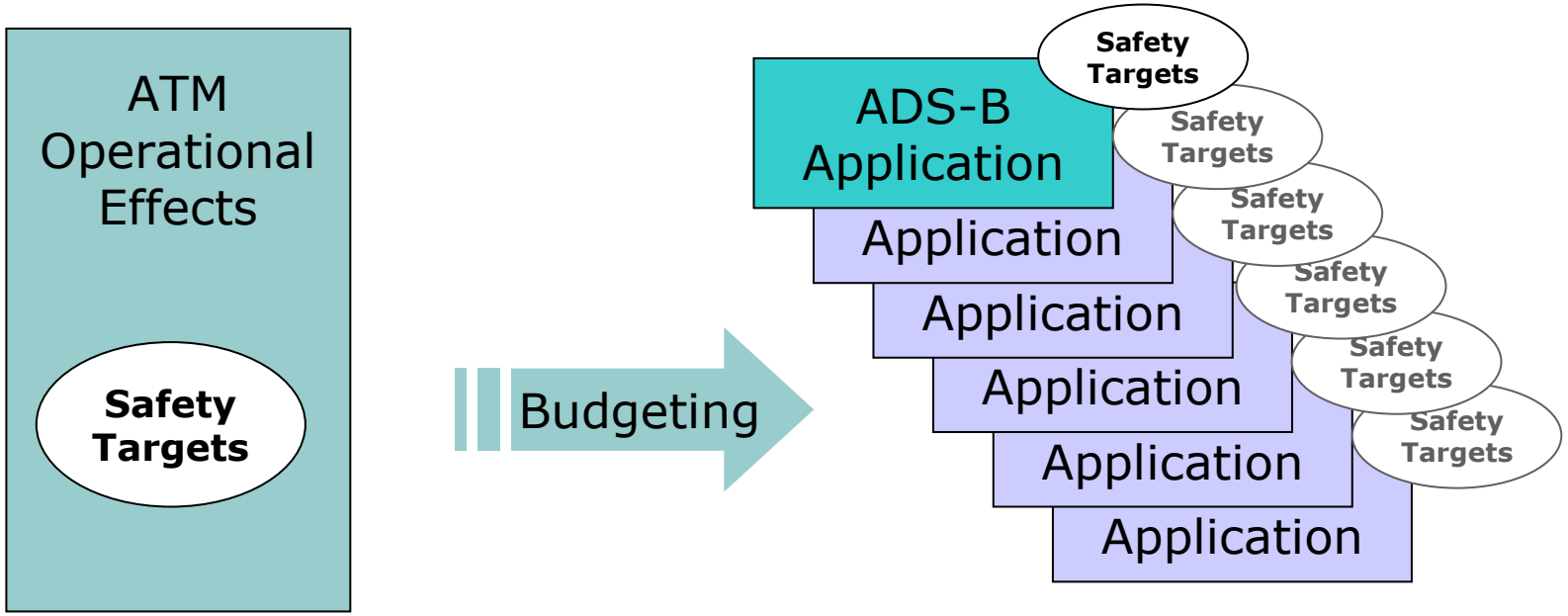


1
2
3
4

OHA Process

ATM Risk budget apportionment

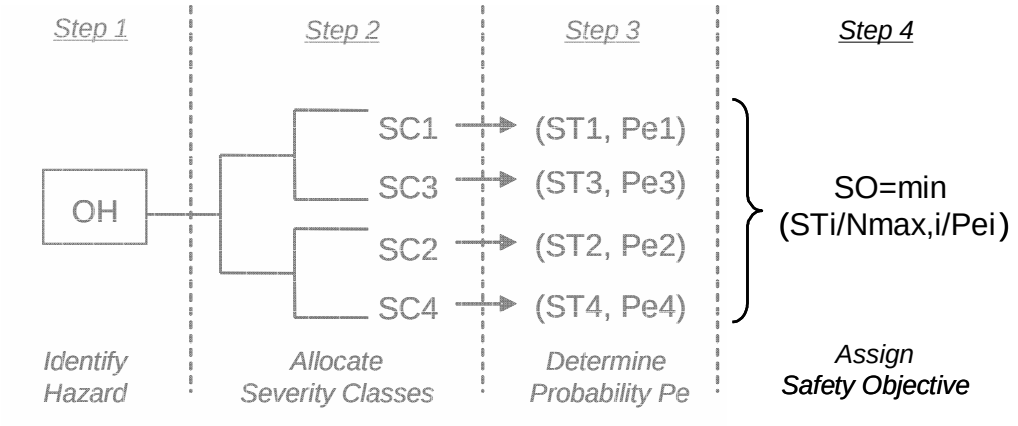




1
2
3
4

OHA Process

4. Safety Objective Assignment

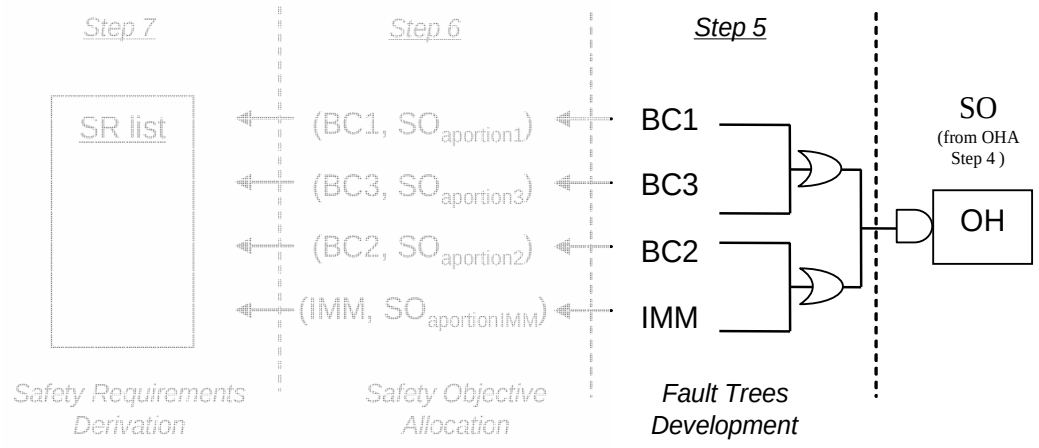


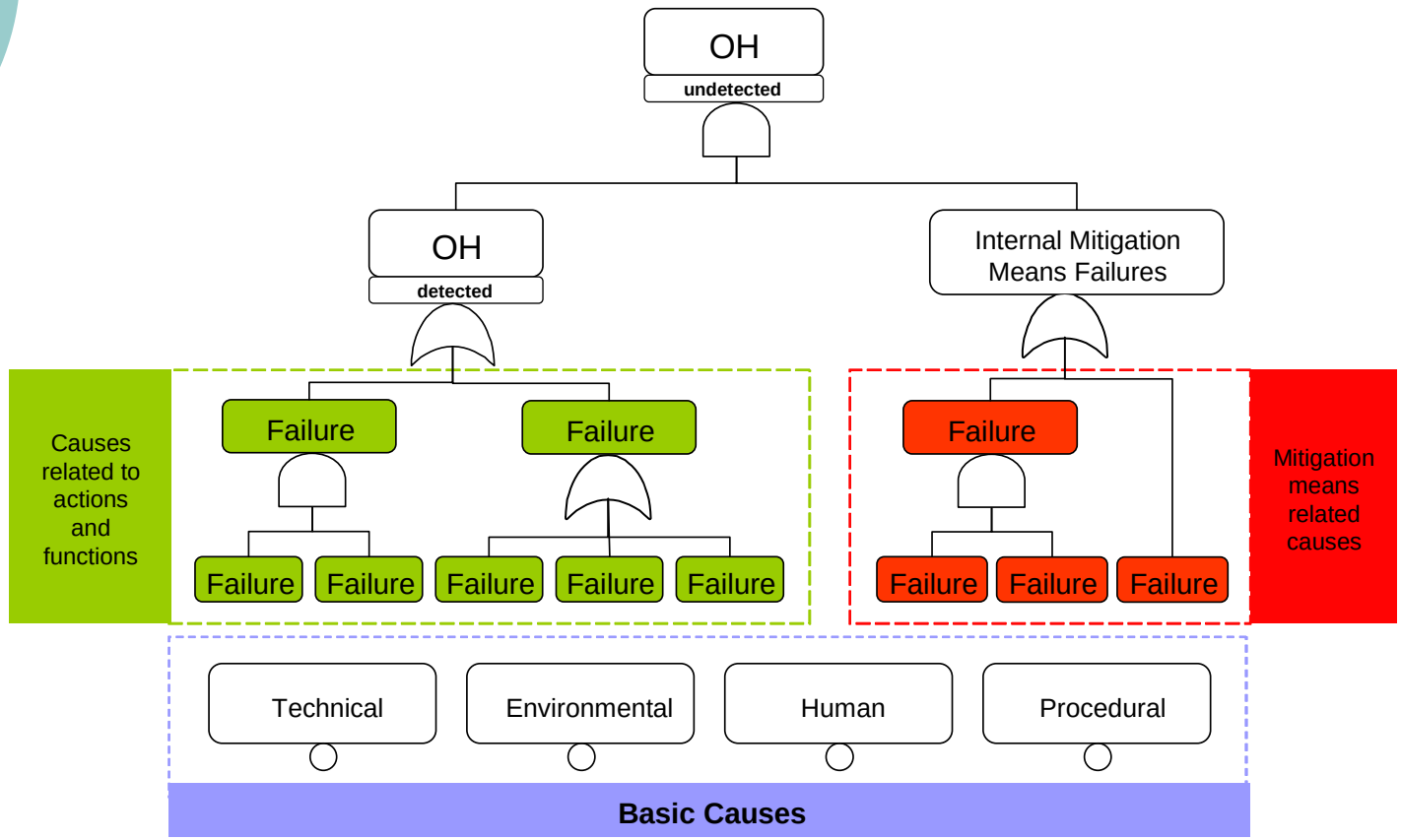
- Calculation of the quantitative **Safety Objective** for each hazard = Specify the maximum acceptable frequency of the hazard.

- Formula applied: $SO_j = \min_i (ST_i / N_{max,i} / Pe_{ij})$, i.e. it takes SO from the most demanding pair (effect, frequency).

ASOR Process

1
2
3
4

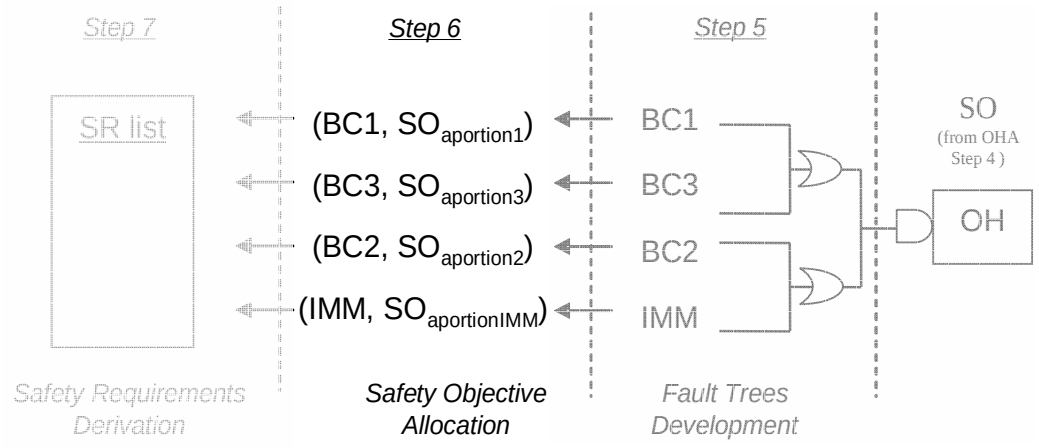


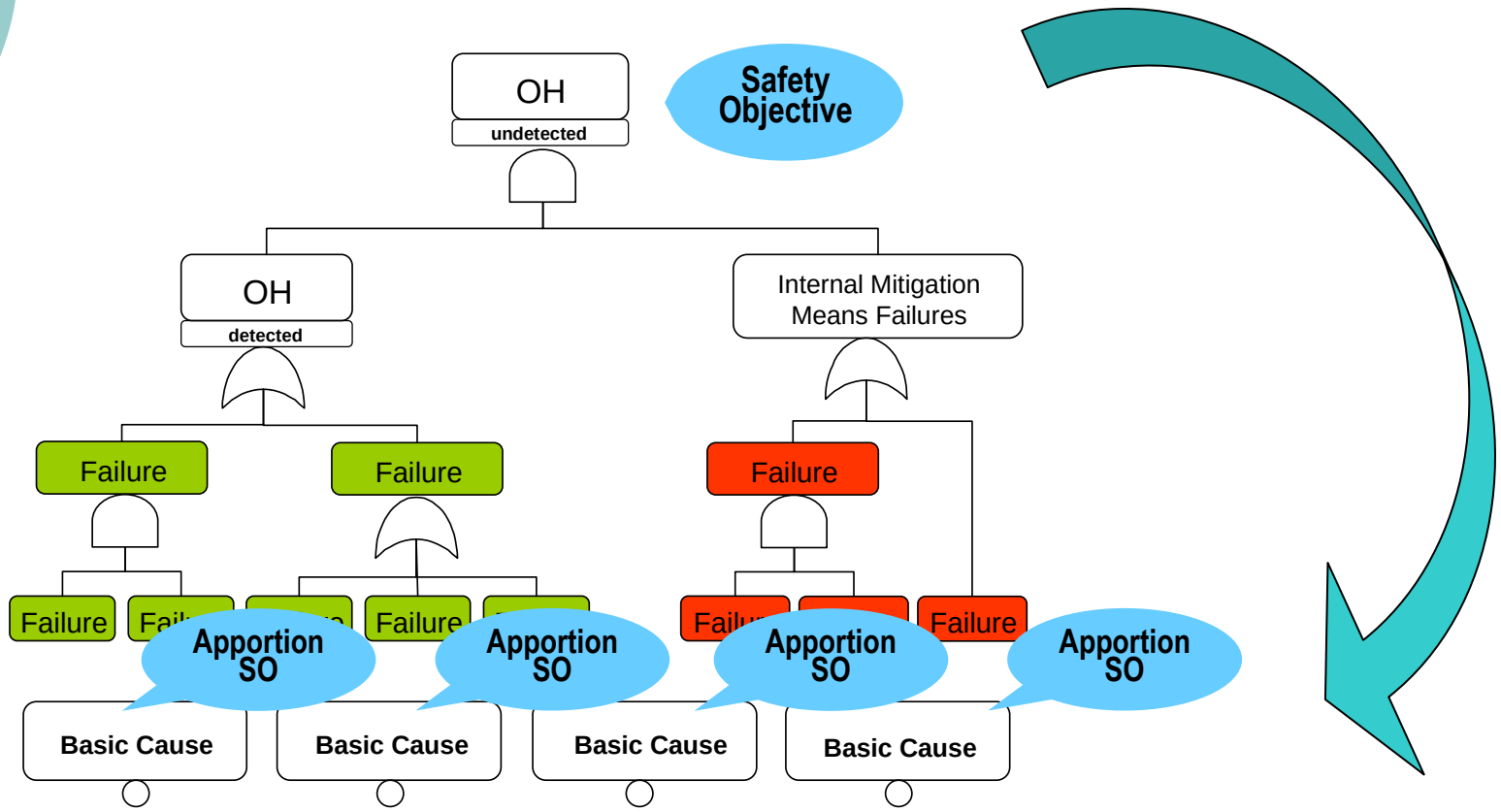


ASOR Process

1
2
3
4

6. Safety Objective Allocation

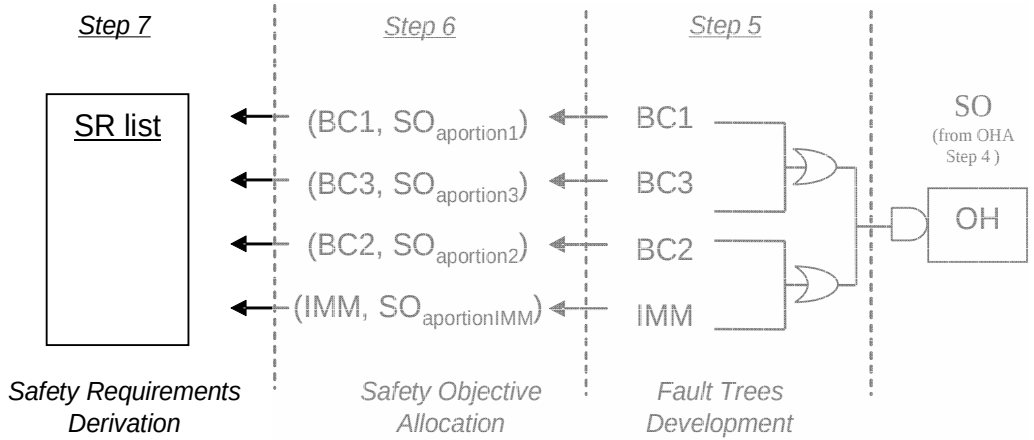


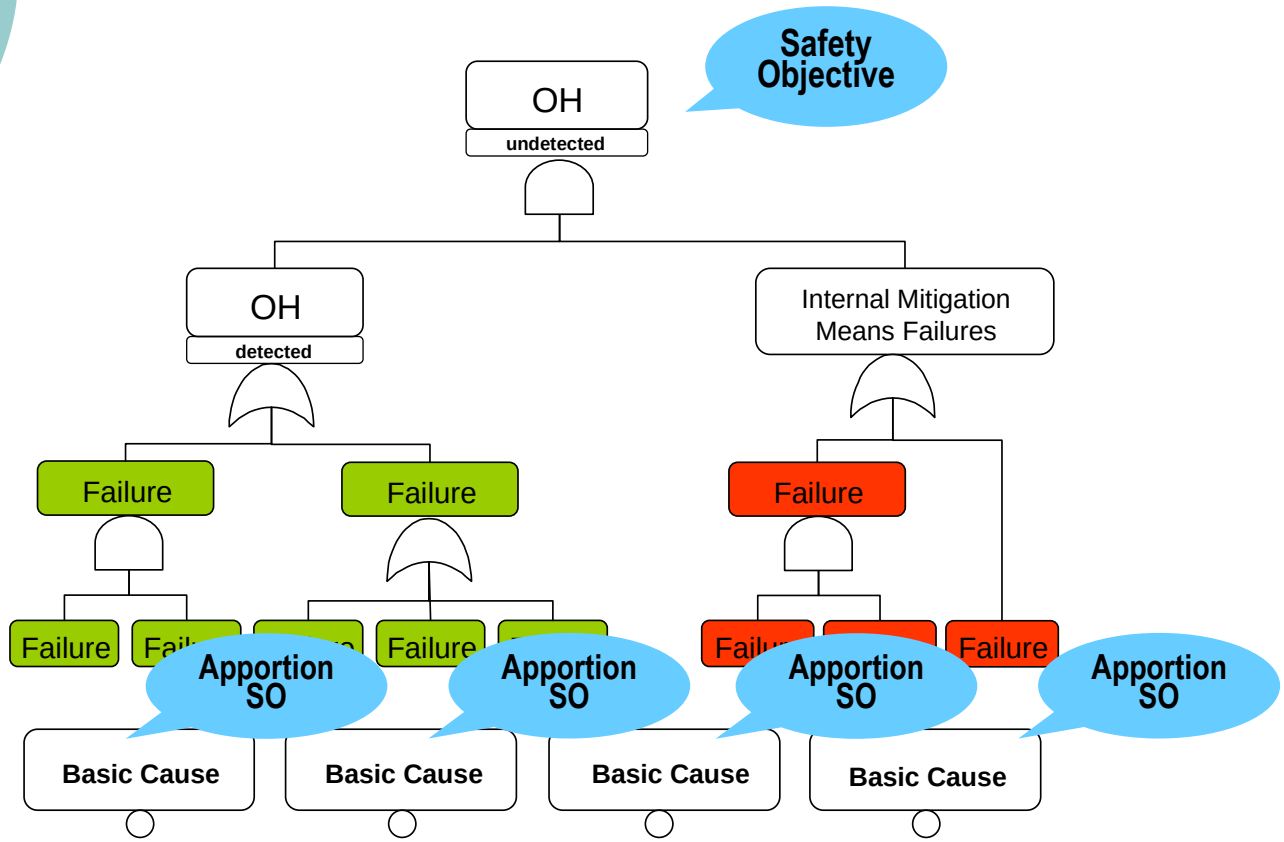


1
2
3
4

ASOR Process

7. Derive Safety Requirements

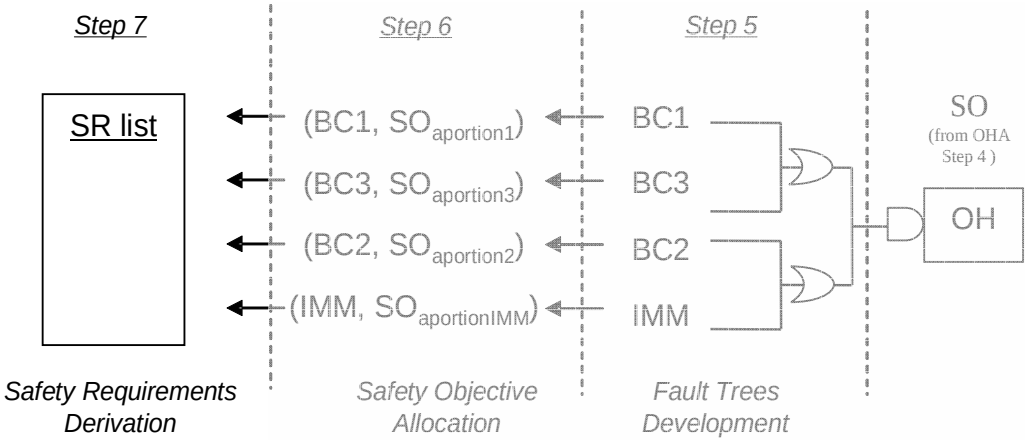


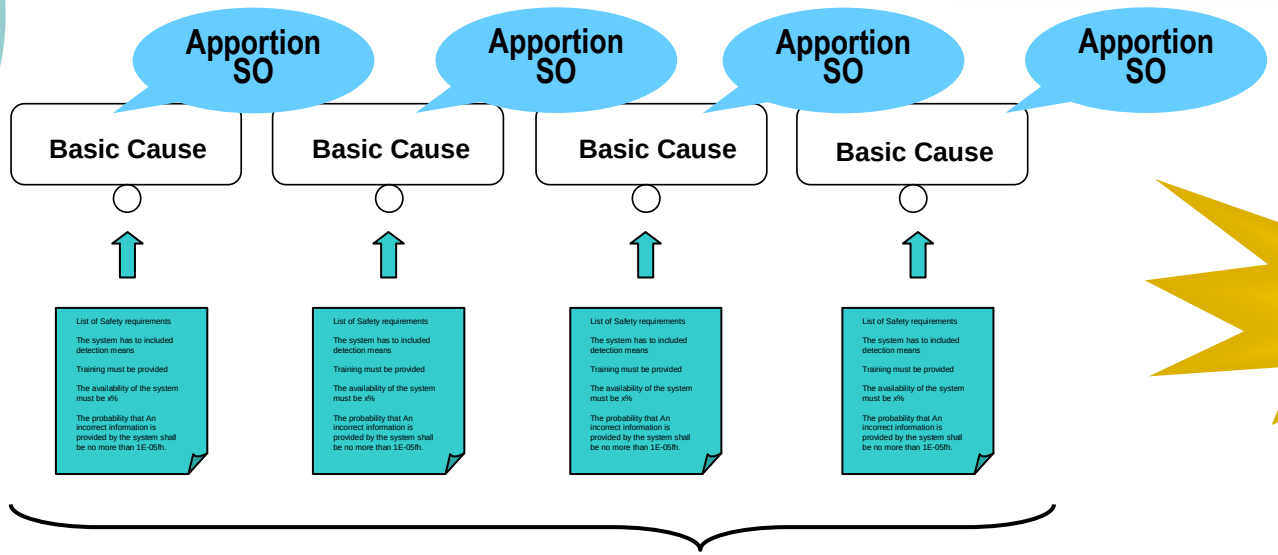


1
2
3
4

ASOR Process

7. Derive Safety Requirements





Safety Requirements

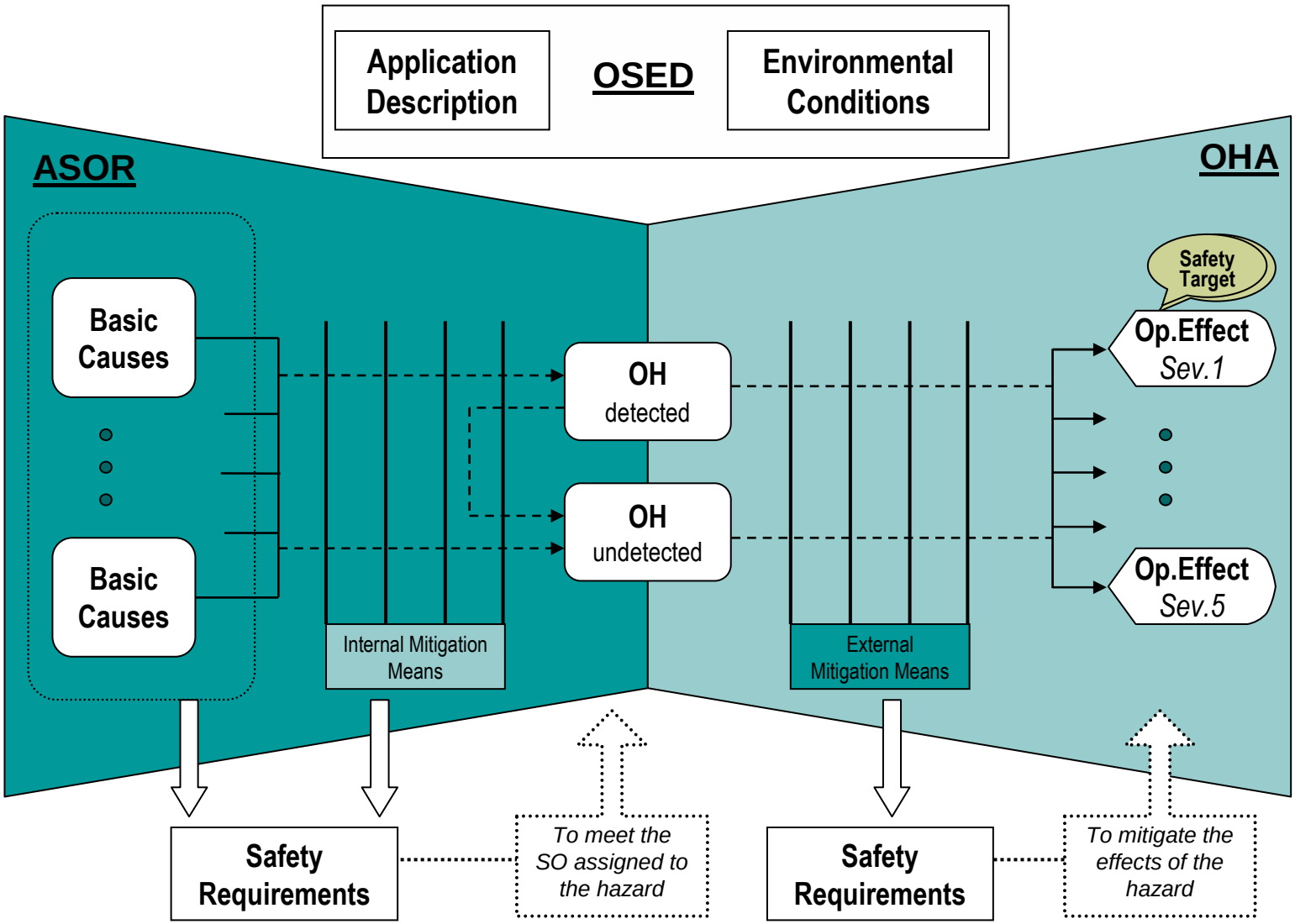
People

Procedures

Equipment

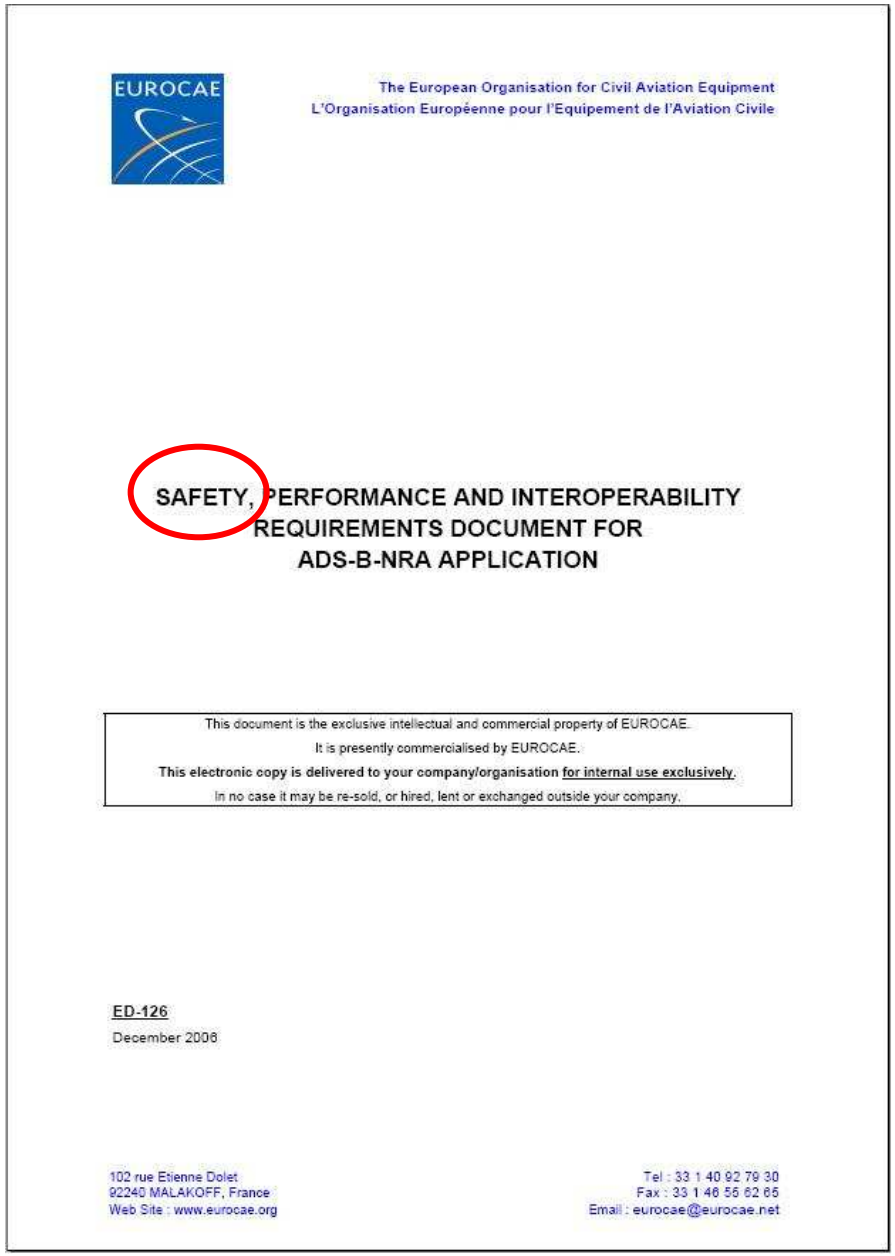
Safety Assessment Overview

1
2
3
4



Case Study

1
2
3
4



The European Organisation for Civil Aviation Equipment
L'Organisation Européenne pour l'Equipement de l'Aviation Civile

SAFETY, PERFORMANCE AND INTEROPERABILITY
REQUIREMENTS DOCUMENT FOR
ADS-B-NRA APPLICATION

ED-126
December 2006

102 rue Etienne Dolet
92240 MALAKOFF, France
Web Site : www.eurocae.org

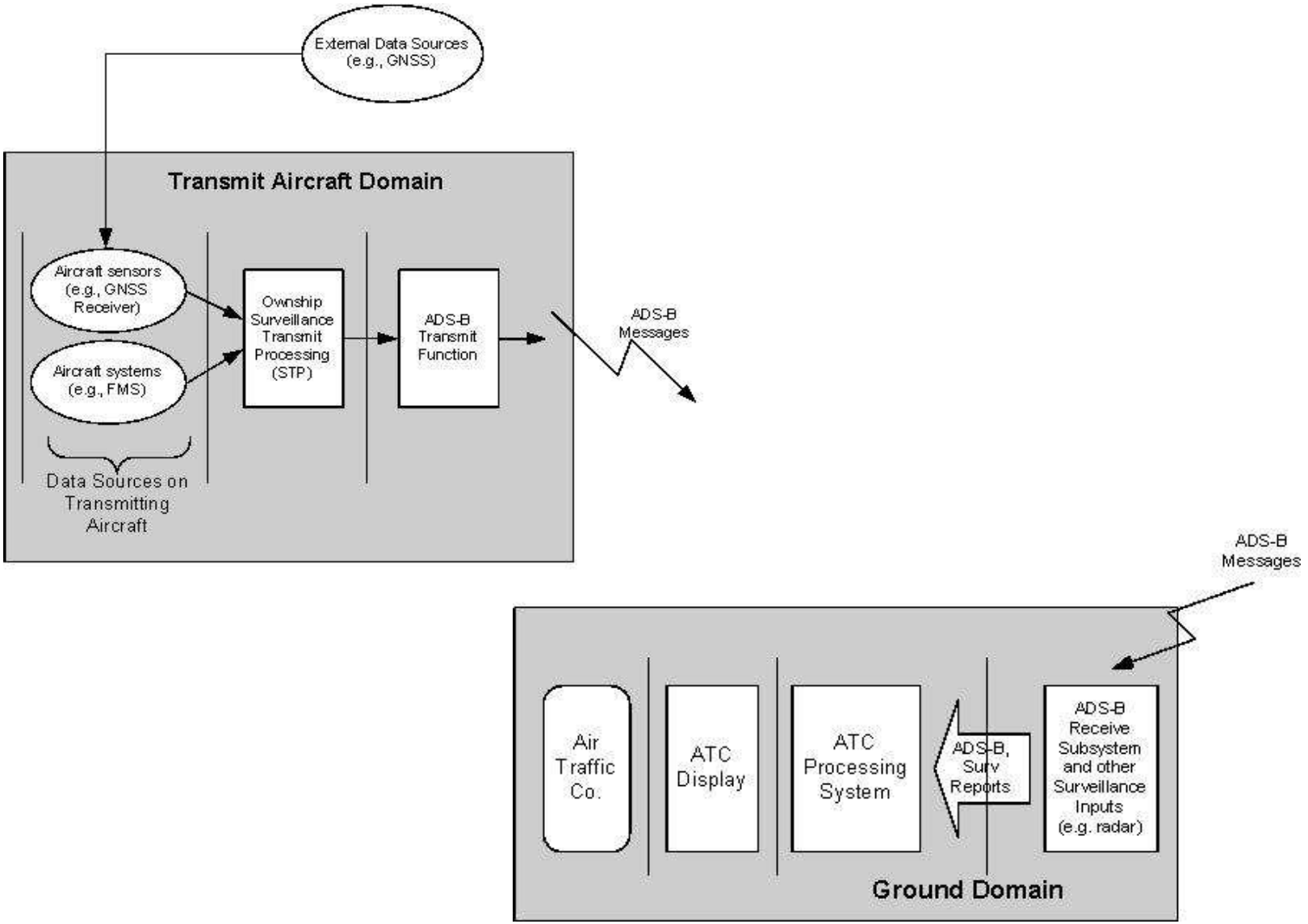
Tel : 33 1 40 92 79 30
Fax : 33 1 46 55 62 65
Email : eurocae@eurocae.net

ED126/DO303

Enhanced Air Traffic Services in Non-Radar Areas using ADS-B surveillance

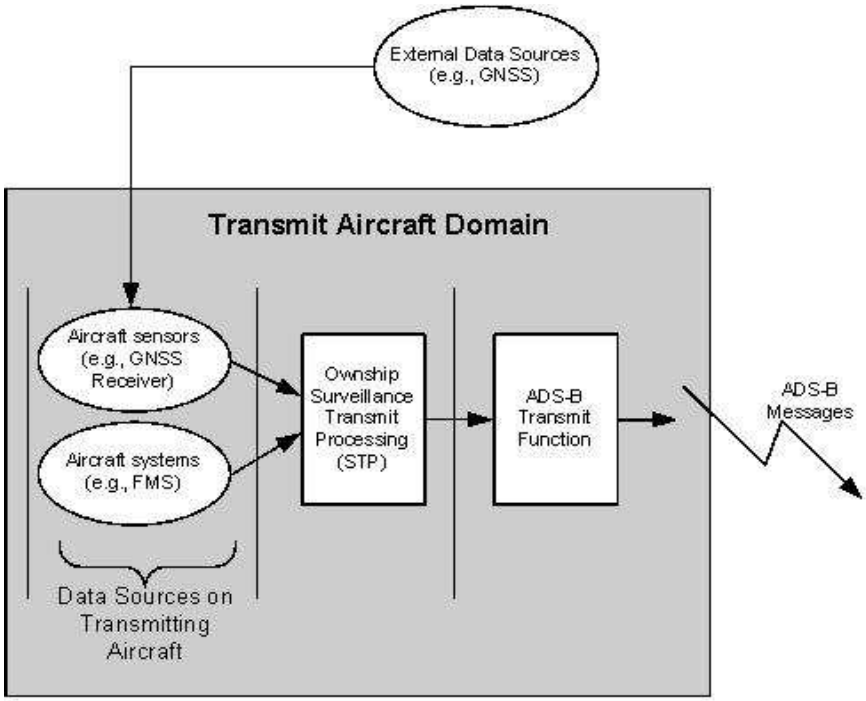
1
2
3
4

Functional description of the system



ADS-B NRA identified Hazards

1
2
3
4

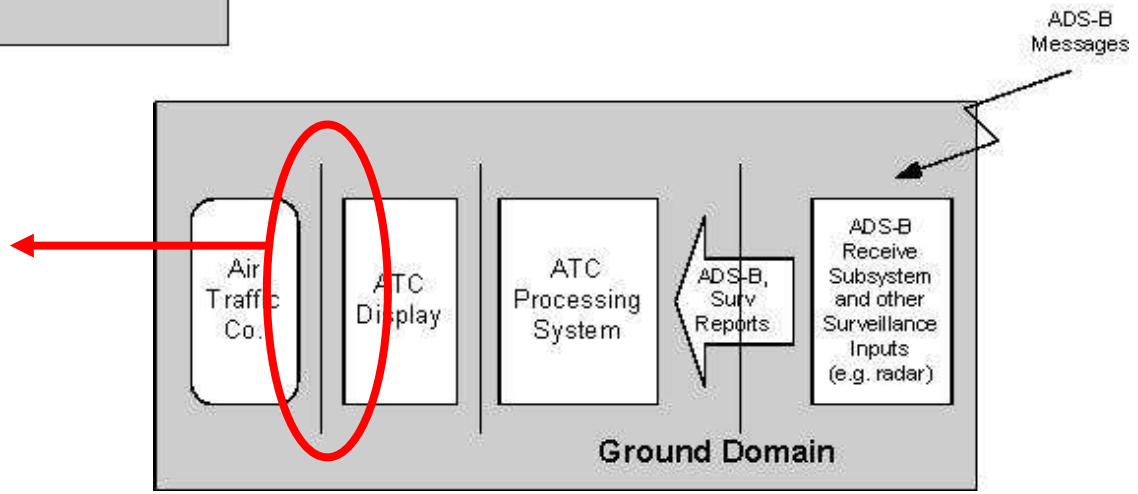


Examples of Hazards

- Controller loses position for one AC
- Incorrect position information for multiple AC is displayed to controller

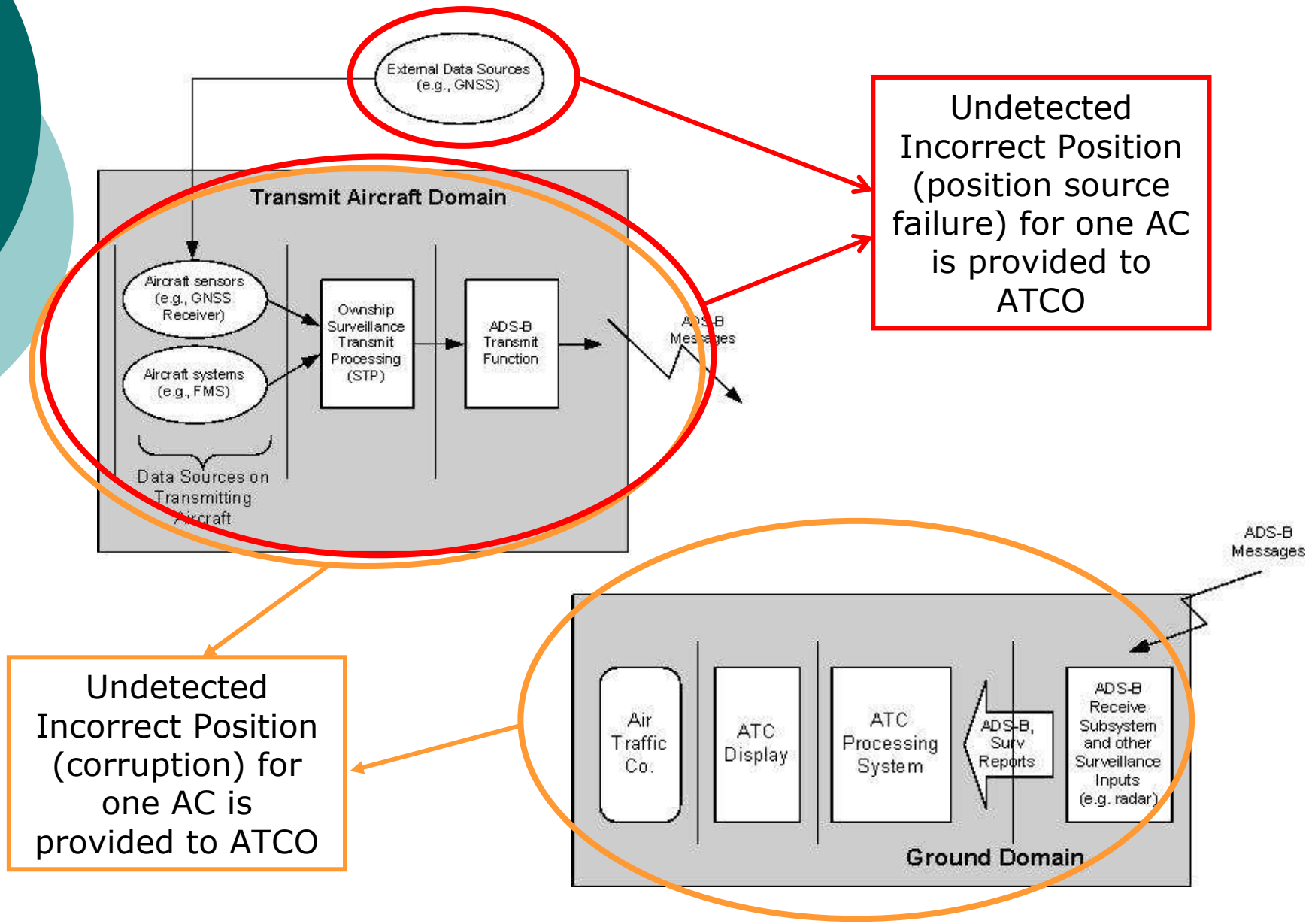
…

Hazards identified at this level



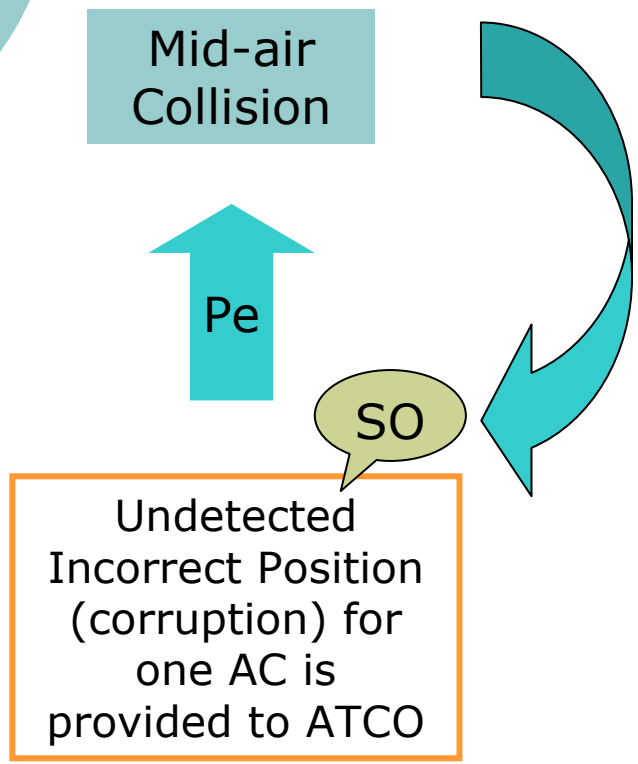
Hazard and Basic Causes: example

1
2
3
4



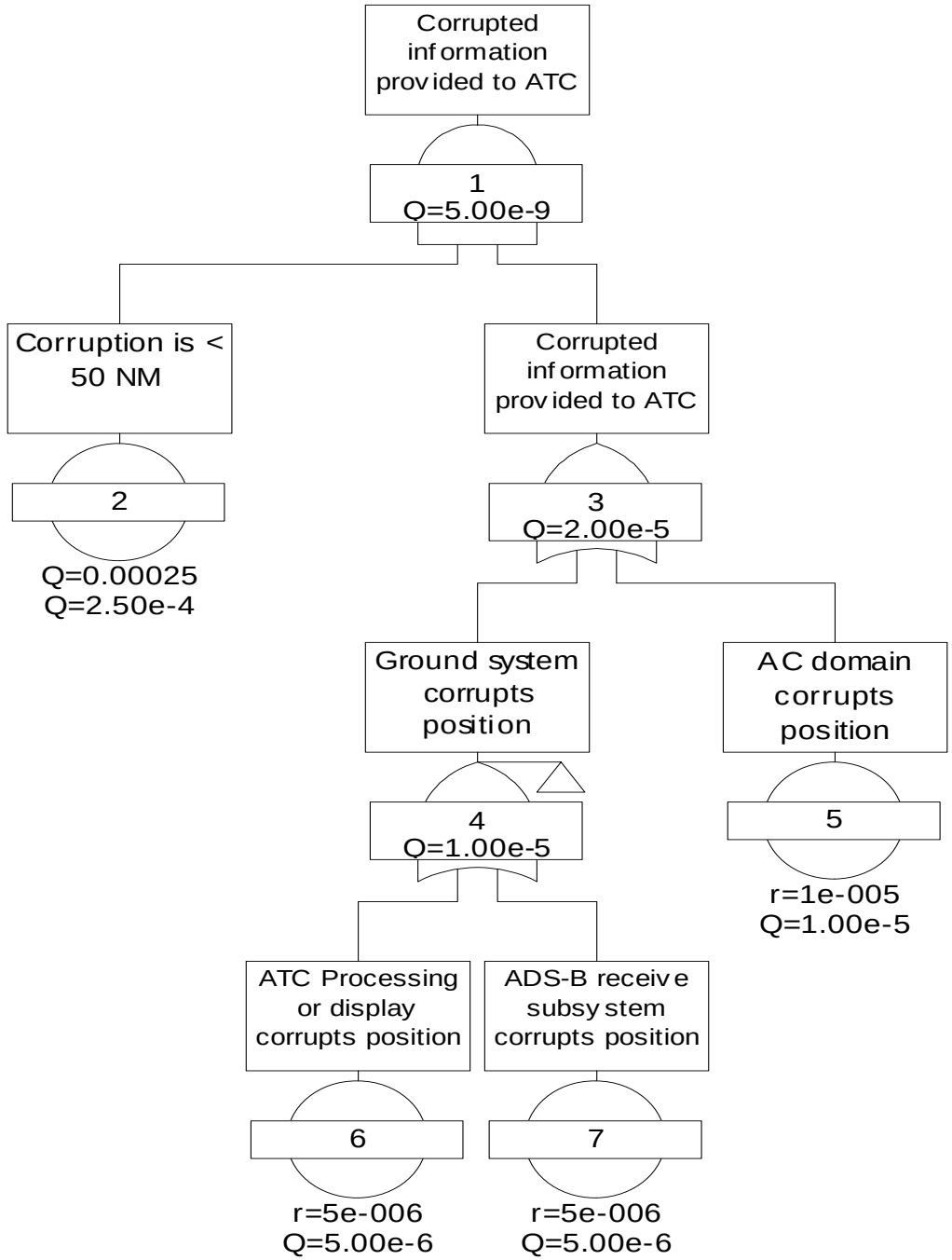
Corrupted Position Information

1
2
3
4



1
2
3
4

Fault Tree

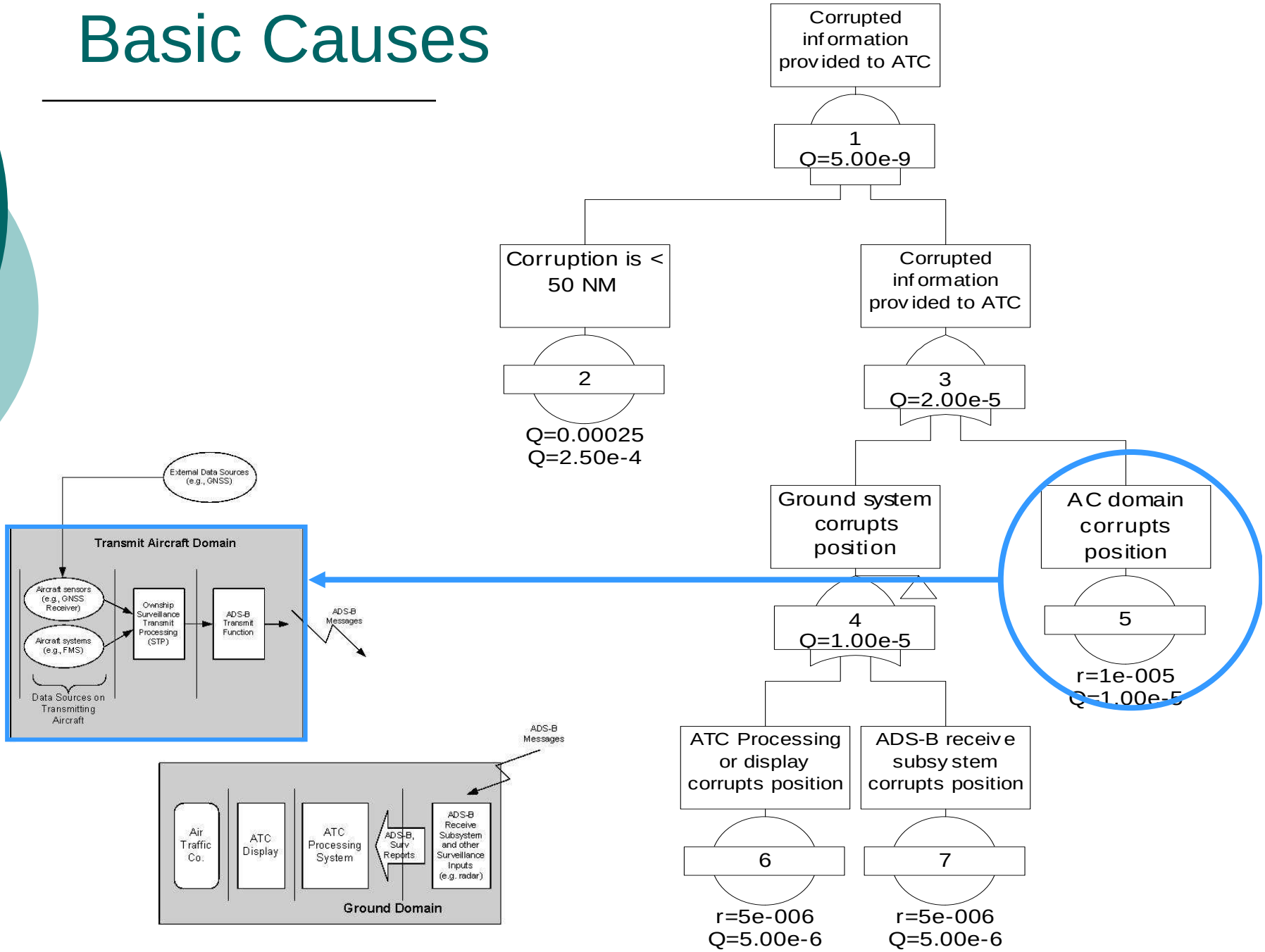


SO

Undetected Incorrect Position (corruption) for one AC is provided to ATCO

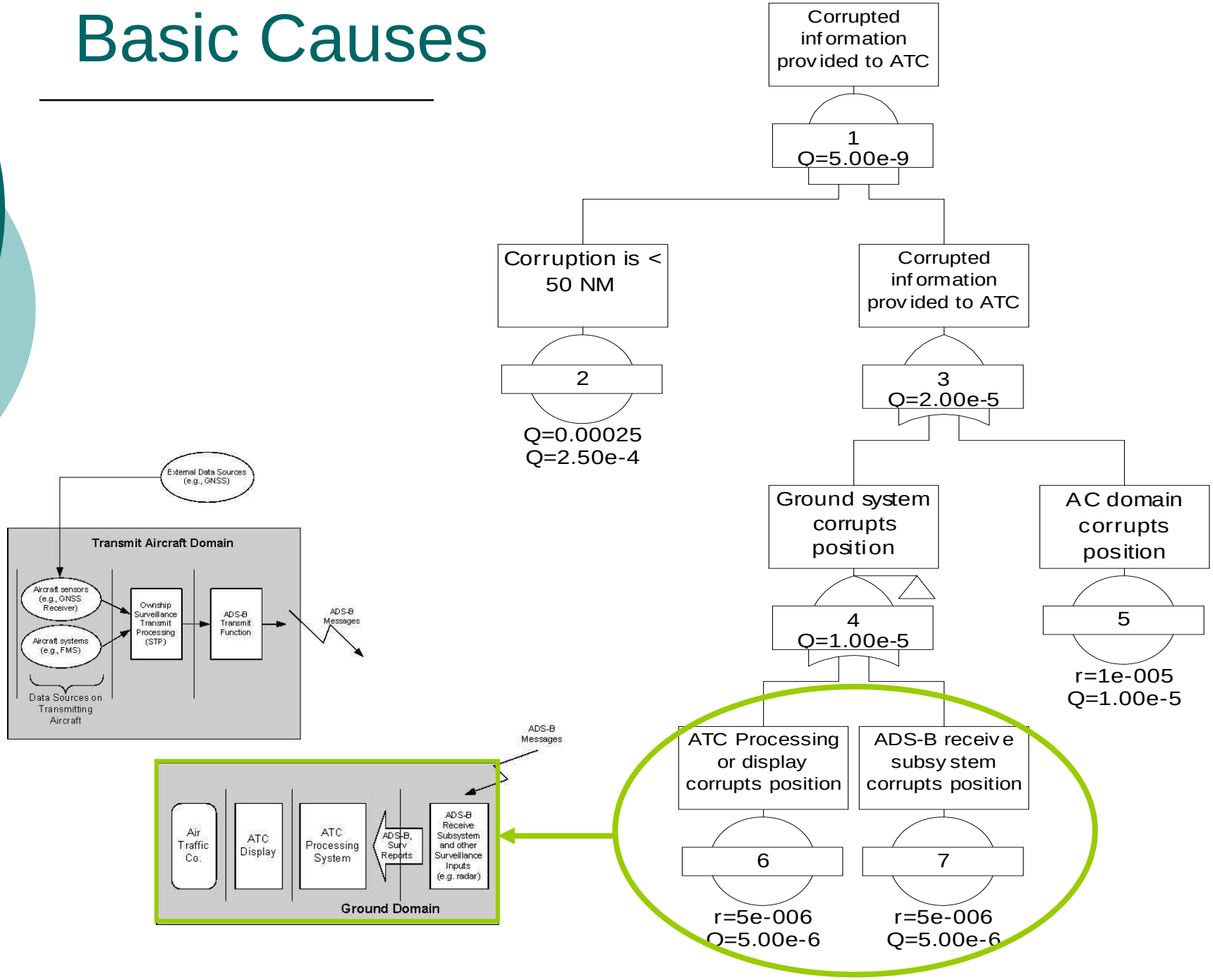
Basic Causes

1
2
3
4



Basic Causes

1
2
3
4

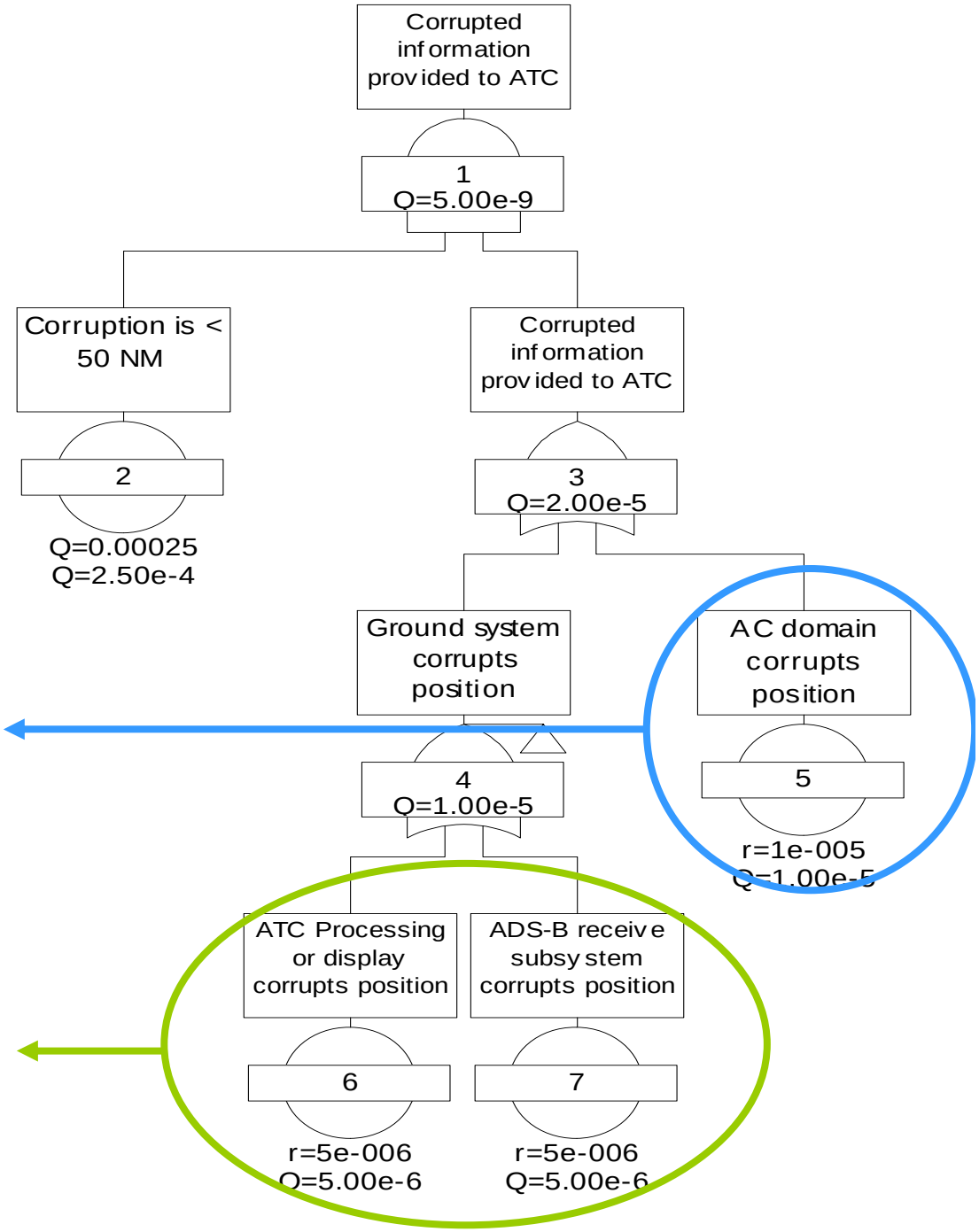


Requirements

1
2
3
4

Safety Requirements on **airborne AND ground** elements, as an input to (for local implementation):

- design assurance level for equipment
- design configuration
- etc.

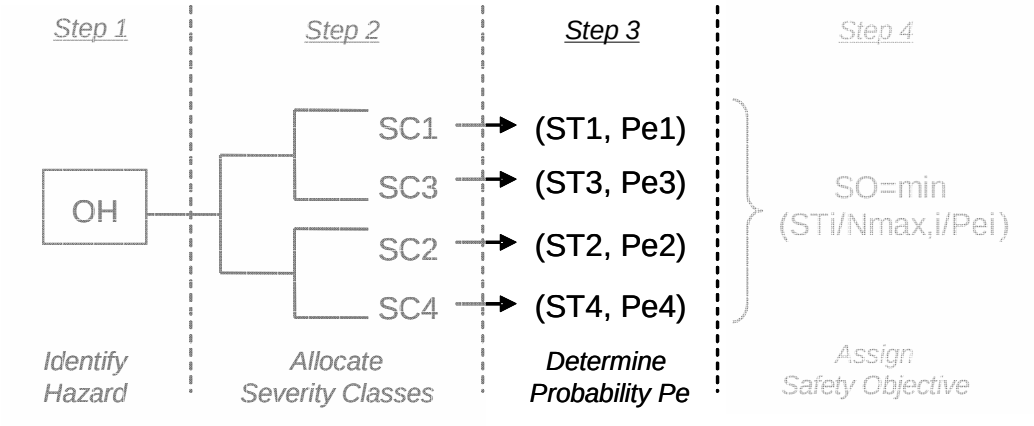


Conclusions

1
2
3
4

- Joint process between US and Europe
- End to end safety process covering airborne and ground domains, operational and technical part
- Used on NRA DO 303/ED 126 and will ultimately contribute to aircraft certification and deployment for ADS-B
- The approach is expected to be re-used in local implementations
- Will be used (and refined) for next to come ADS-B standards to be delivered by RFG

OHA Process



ATM Risk budget apportionment

Units

ST ATM	[fh] or [flight]	[ATSUh] en route	[ATSUh] TMA
1	1E-08	1E-07	1E-08
2	1E-05	1E-04	1E-05
3	1E-04	1E-03	1E-04
4	1E-02	1E-01	1E-02

ATM

Nmax per SC	[ATSUh] en route	[ATSUh] TMA
20	5E-09	5E-010
25	4E-06	4E-07
35	3E-05	3E-06
45	2E-03	2E-04

Application

Risk Apportionment