Safety Assessment Training Workshop

Major Exercise - Briefing:
- ALC in LV
or
- FARADS

Derek FOWLER
JDF Consultancy LLP

February 2008

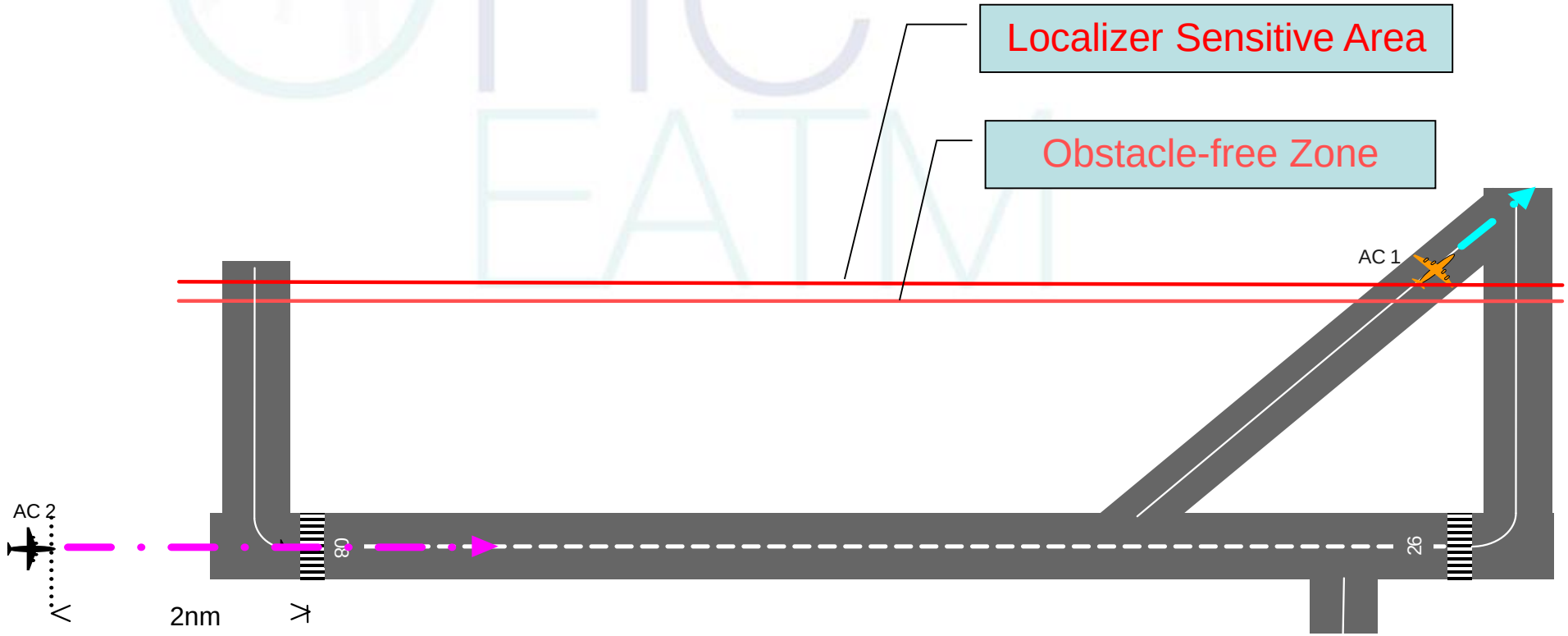
EUROCONTROL

Major Exercise – ALC in LV

- Anticipated Landing Clearances in Low-visibility MLS / GBAS Operations

New-technology approach / landing aids – potential benefits in reducing delays

Current Operations - ILS Cat II/III Landing



Landing Clearance given such that LSA / OFZ protected

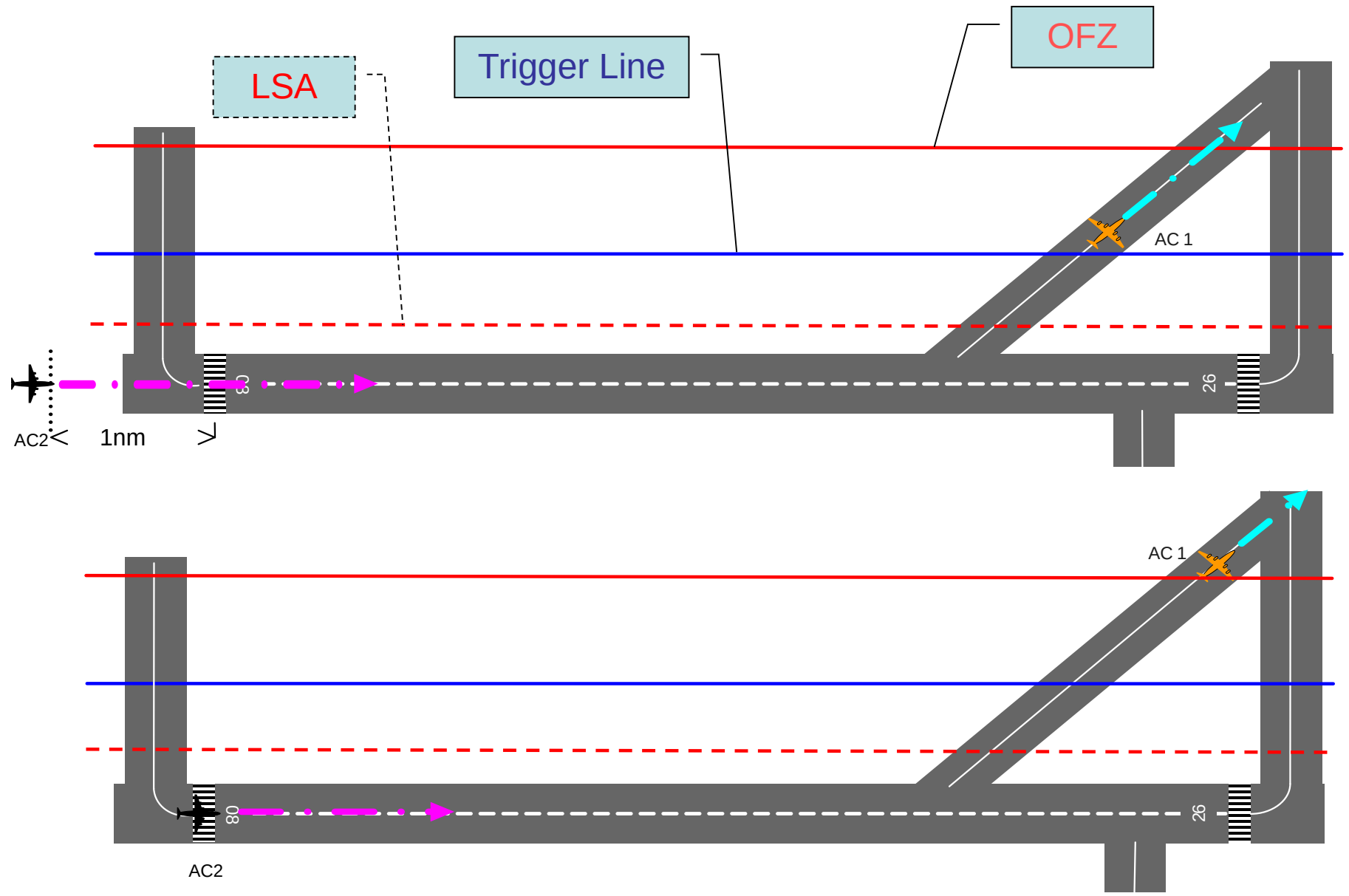
EUROCONTROL

Current Operations (ILS Cat II/III)

- Landing clearance to an aircraft on Final Approach (AC2) cannot be given until previous aircraft (AC1) has already cleared the ILS Cat II/III Localiser Sensitive Area (LSA) – normally given before 2nm from THR
- This ensures that the ILS beam is protected for AC2 against reflections etc caused by AC1
- For ILS Cat II/III, the LSA is bigger than the airfield Obstacle-free Zone (OFZ)
- Thus protecting the LSA for AC2 ensures that the OFZ is also protected – ie whether AC2 lands, or goes around, it cannot hit AC1

EUROCONTROL

MLS / GBAS Cat II/III Landing Clearance



MLS / GBAS Operations

- For MLS / GBAS Cat II/III landings, the LSA is much smaller than the OFZ
- Landing clearance to an aircraft on Final Approach (AC2) cannot be given until previous aircraft (AC1) has cleared “Trigger Line” – normally given before 1nm from THR
- Trigger Line fixed on Controllers A-SMGCS display so that:
  - AC1 will have cleared the LSA by the time AC2 reaches 1nm before THR
  - AC1 will have cleared the OFZ by the time AC2 has crossed the THR

EUROCONTROL

ALC Tasks

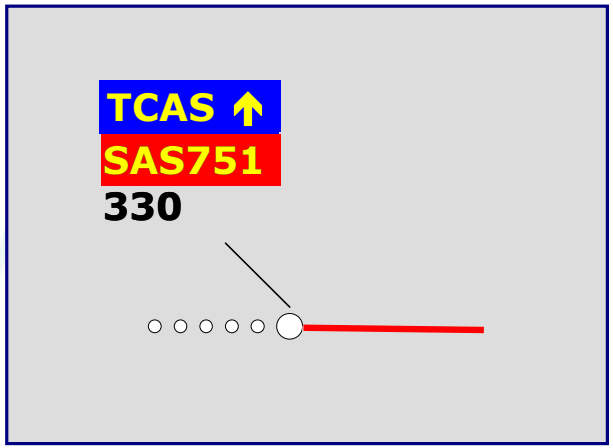
1. Determine a suitable set of Safety Criteria
2. Explain why ALC in LV is intrinsically safe, and outline the key parameters that make it so – Arg1.1
3. Derive a few Safety Requirements covering:
   - the display of the Trigger Line
   - actions required of the Controller
   - actions required of the Flight Crew

   } Arg1.2
4. Suggest how you would get Evidence for Arg1.3
5. Give examples of abnormalities that would be appropriate to ALC under Arg1.4
6. What Hazards should be considered under Arg1.5

EUROCONTROL

Major Exercise - FARADS

- Feasibility of RA Downlink Study



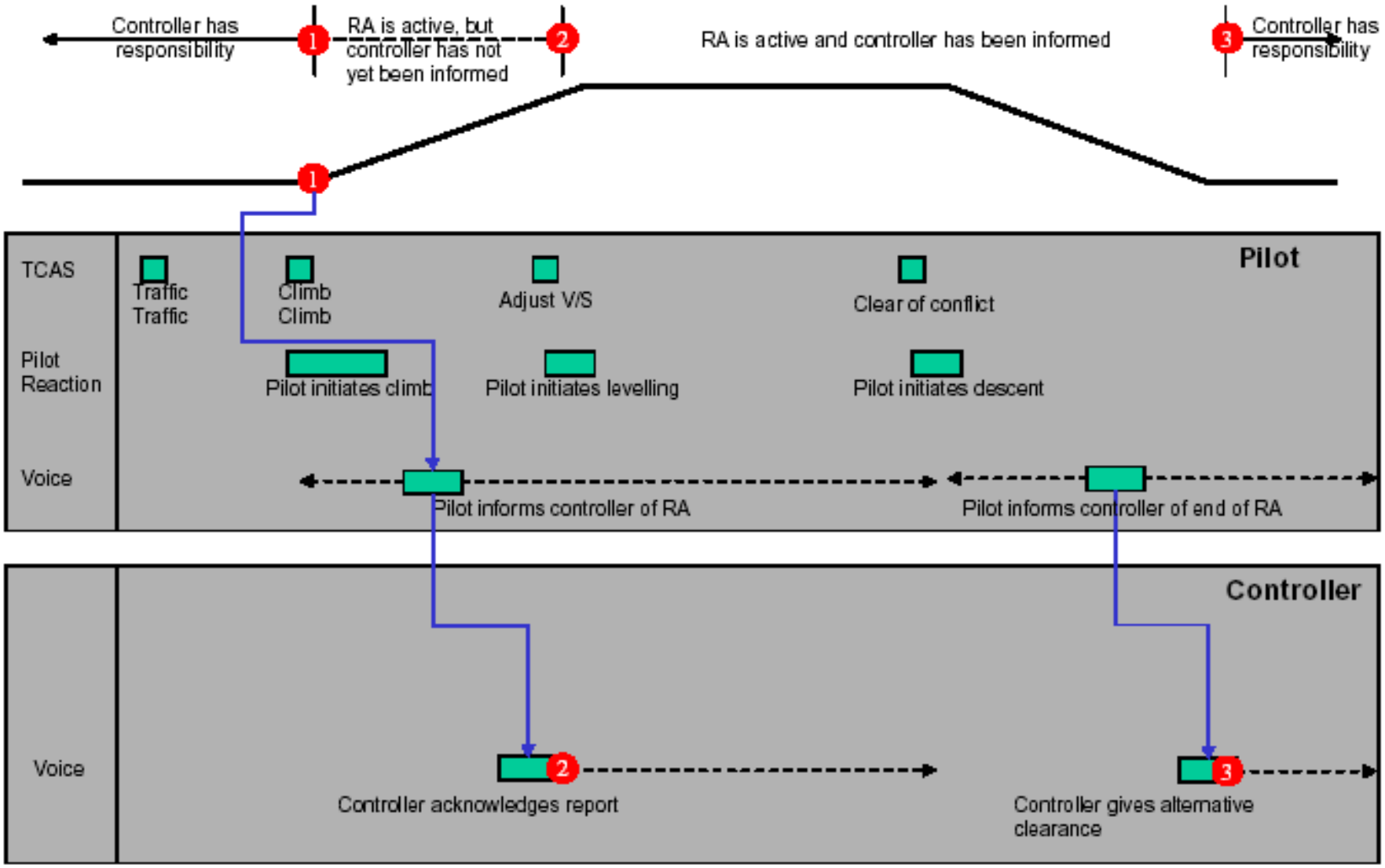
EUROCONTROL

FARADS

- Eurocontrol study into ACAS RA downlinking
- Response to the Überlingen accident in 2002
- Objective is to assess the technical and operational feasibility of displaying ACAS RA information on CWPs
- Possible operational benefits include:
  - improved ATCO situational awareness - helping them to anticipate aircraft manoeuvres
  - reduced likelihood of contradictory ATC clearances to the aircraft in RA incident
  - reduced risk of subsequent conflicts through better information and planning

EUROCONTROL

Pre-FARADS Situation



NOTES:

1. At this point, controller no longer has legal responsibility for separation
2. At this point the controller is informed of the RA, and realises that he no longer has separation responsibility
3. At this point the controller regains separation responsibility

Some Human Considerations

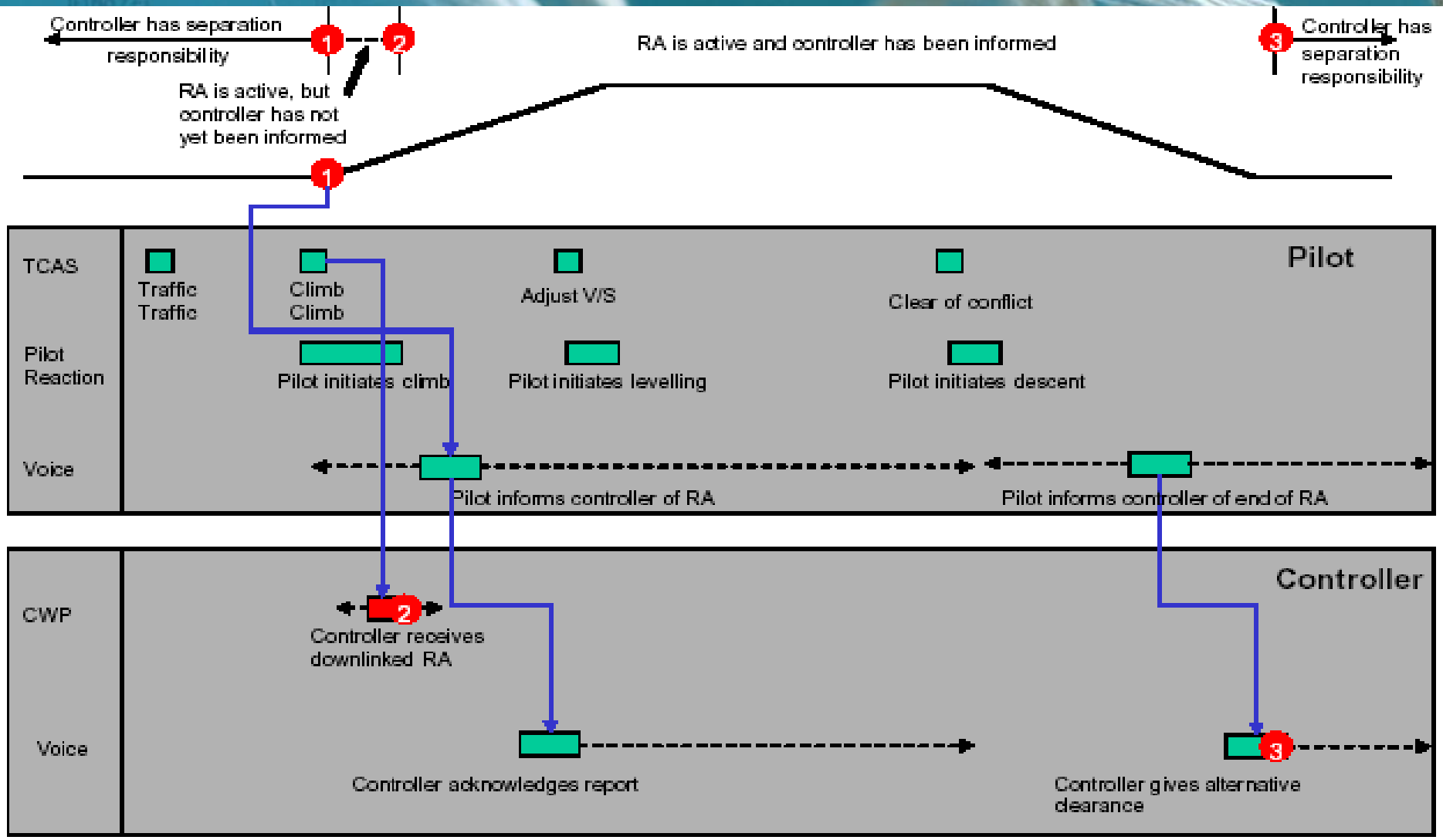
Cockpit Audible Alert	ICAO Phraseology to Report RA	CWP RA
Adjust vertical speed, adjust	No specific phraseology prescribed	TCAS –
Monitor vertical speed	No specific phraseology prescribed	TCAS
Climb, climb Climb, crossing climb Increase climb… Maintain vertical speed, maintain * Maintain vertical speed, crossing maintain *	[callsign] TCAS CLIMB	TCAS ↑
Descend, descend Descend, crossing descend Increase descend… Maintain vertical speed, maintain * Maintain vertical speed, crossing maintain *	[callsign] TCAS DESCENT	TCAS ↓
Climb, climb now…	[callsign] TCAS CLIMB	TCAS (↓) ↑
Descend, descend now…	[callsign] TCAS DESCENT	TCAS (↑) ↓
Clear of conflict	[callsign] TCAS CLIMB (or DESCENT) COMPLETED (*assigned clearance*) RESUMED	[none]

Possible Technologies

- in areas covered by a Mode S ground infrastructure, Mode S Report is the best method for RA downlink;
- in areas not covered by a Mode S ground infrastructure, Extended Squitter is the best method for RA downlink (assuming it can be economically implemented as part of an ADS-B system);

EUROCONTROL

FARADS Situation



NOTES:

1. At this point, controller no longer has legal responsibility for separation
2. At this point the controller is informed of the RA
3. At this point the controller regains separation responsibility

Current

Additions for OC7

FARADS Tasks

1. Determine a suitable set of Safety Criteria
2. Explain why RA Downlink is intrinsically safe, and outline the key parameters that make it so – Arg1.1
3. Derive a few Safety Requirements covering:
   - the display of the RA for the Controller
   - actions required of the Controller
   - actions required of the Flight Crew

   } Arg1.2
4. Suggest how you would get Evidence for Arg1.3
5. Give examples of abnormalities that would be appropriate to RA Downlink under Arg1.4
6. What Hazards should be considered under Arg1.5

EUROCONTROL

Safety Assessment Training Workshop

ALC in LV – Suggested Solution

Derek FOWLER
JDF Consultancy LLP

February 2008

EUROCONTROL

Safety Criteria

- The risk of an accident shall be:
  - no greater than for ILS Cat II/III operations (with A-SMGCS)
  - reduced as far as reasonably practicable

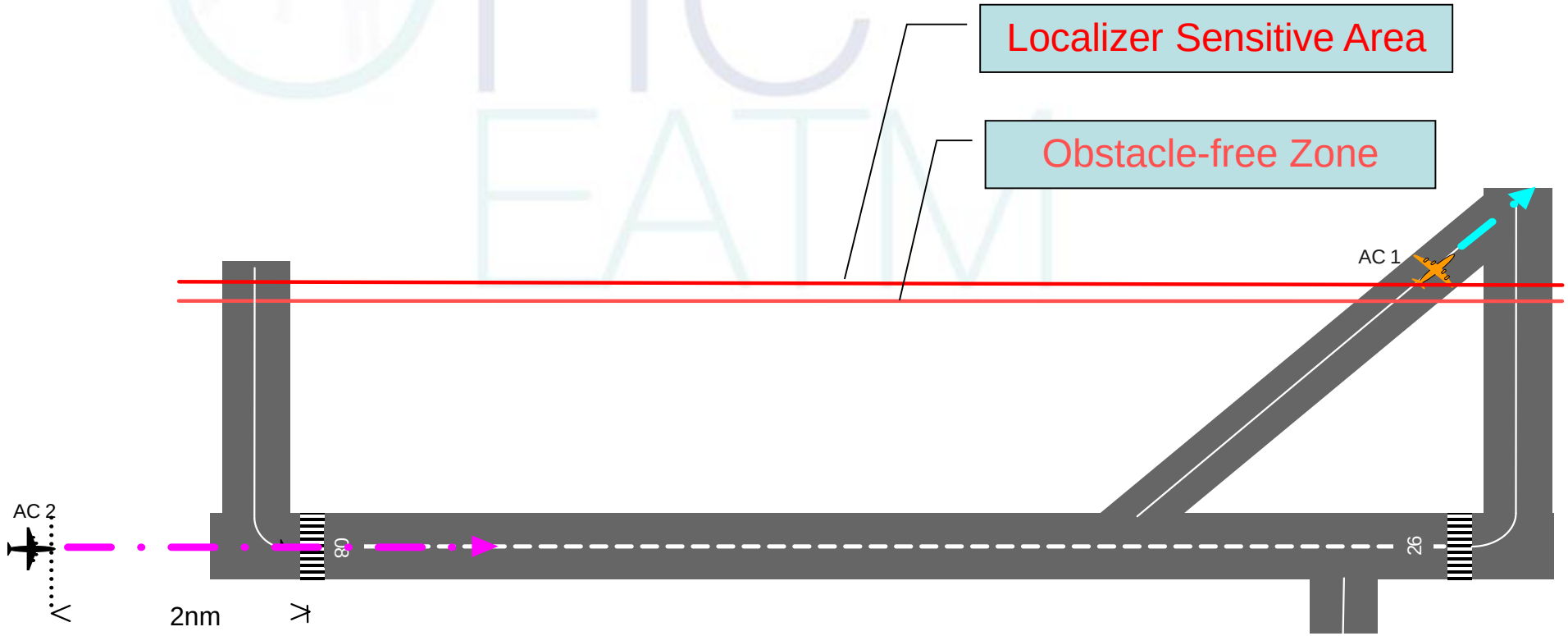
EUROCONTROL

Arg1.1 – Intrinsic Safety

Potential to satisfy the Safety Criteria

EUROCONTROL

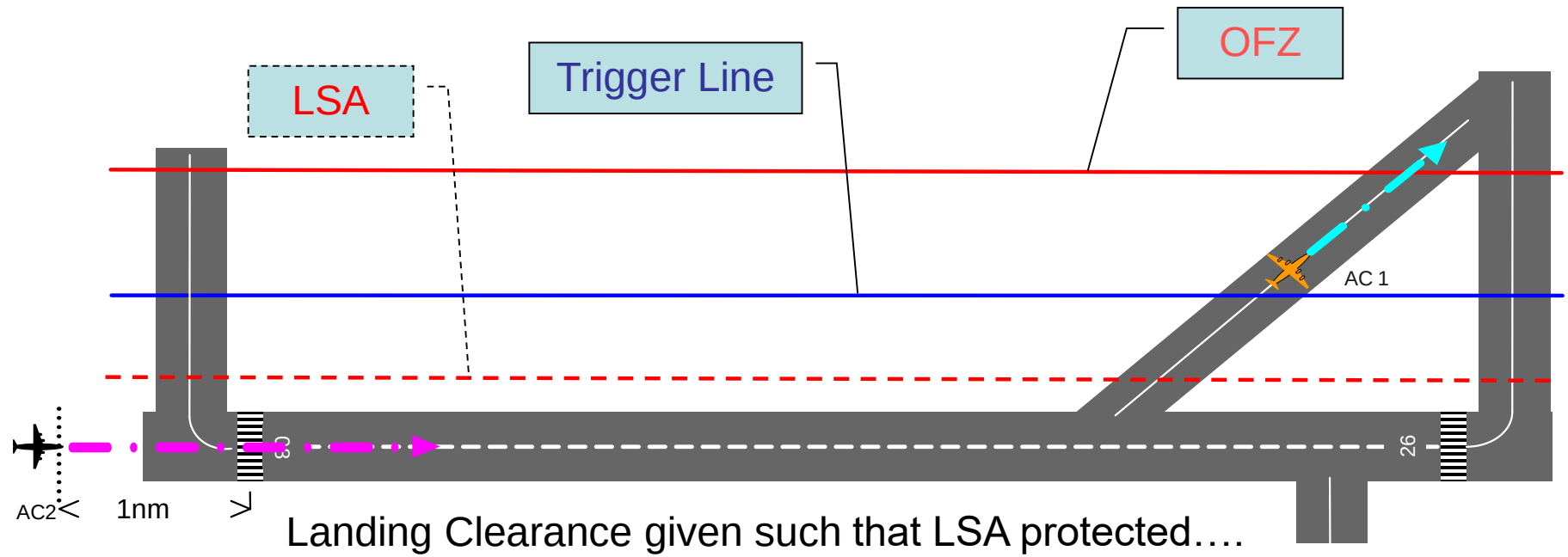
Current Operations - ILS Cat II/III Landing



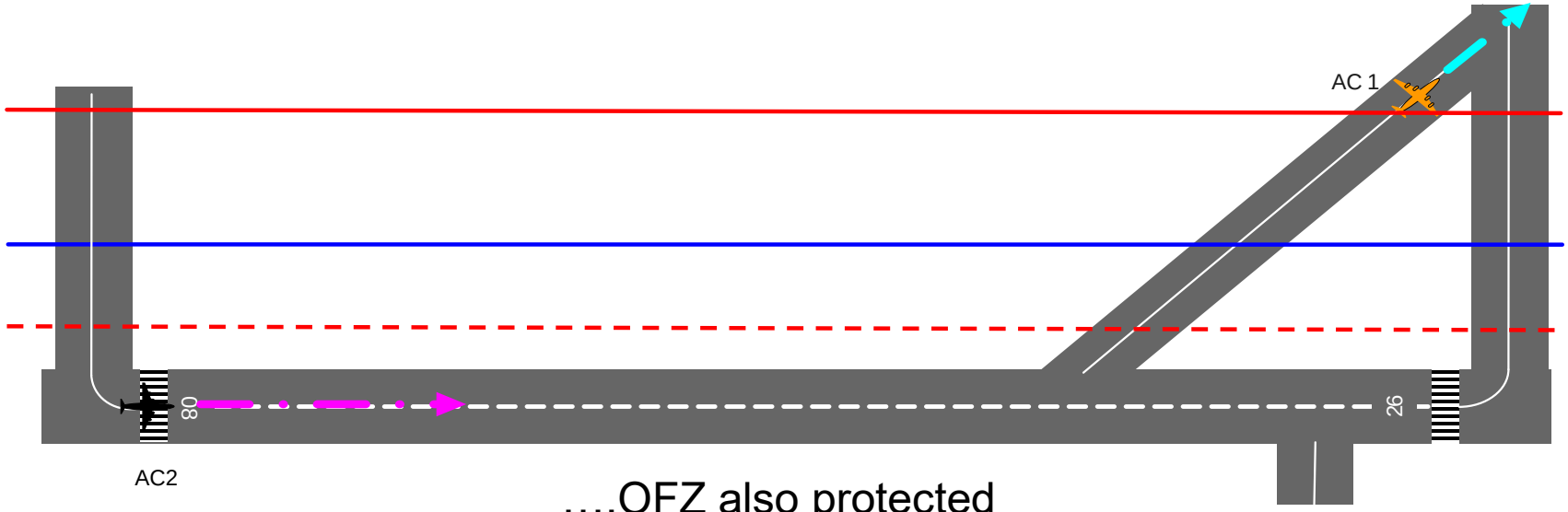
Landing Clearance given such that LSA / OFZ protected

EUROCONTROL

MLS / GBAS Cat II/III Landing Clearance



Landing Clearance given such that LSA protected….



….OFZ also protected

Therefore…

- ALC in LV has potential to be safe (cf ILS Cat II/III) because:
  - (reduced) Localizer Sensitive Area is still protected
  - Obstacle-free Zone is still protected
- Key functionality / parameters :
  - the time for AC1 to taxi from the Trigger Line until clear of OFZ must always be less than the time for AC2 fly the last 1 nm before THR
  - the Trigger Line must be outside the MLS/GBAS LSA
  - AC1 must continue taxiing until clear of OFZ
  - AC2 must be given clearance by 1 nm from THR, or go around, to achieve:
    - stabilized landing; or
    - safe Missed Approach

These are the “foundations”, but are not the whole building!

EUROCONTROL

Arg1.2 – Design Completeness

EUROCONTROL

Examples of Initial Safety Requirements (1)

- Trigger Line shall be displayed on the **Controller's HMI**
- The minimum distance between the **Trigger Line** and the runway edge shall be determined as follows:
  - Trigger Line shall always be further from the runway edge than the MLS/GBAS LSA
  - Trigger Line shall be positioned such that the time for AC1 to taxi (or be towed) from the Trigger Line until it is clear of the OFZ is always less than the time needed for AC2 to cover the last 1 nm of its Final Approach).
  - Trigger Line position shall take full account of the slowest average speed of an aircraft in taxiing (or being towed) between the Trigger Line and the edge of the OFZ, and the fastest average groundspeed of an aircraft on Final Approach
  - Trigger Line position shall be determined for largest aircraft using airport
  - Trigger Line position shall take full account of the accuracy / resolution of the display of aircraft position and the Trigger Line

Examples of Initial Safety Requirements (cont..)

- **Controller** shall not issue a landing clearance to an aircraft until preceding aircraft has crossed the Trigger Line
- **Controller** shall issue a landing clearance to an aircraft by the time it has reached 1nm from the runway THR (at the latest), or issue a go-around
- **Aerodrome Procedures** shall require **Pilots** to go around at 200ft above THR if no landing clearance received from ATC
- **Aerodrome Procedures** shall require **Pilots** to continue taxiing until clear of the OFZ
- **Aerodrome Procedures** shall require **Pilots** to inform the Controller if forced to stop before clear of the OFZ
- **Aerodrome Procedures** shall require **Pilots** to transmit RT communication on TWR frequency when crossing active runway

Techniques for Arg1.3 – Design Correctness

- Scenario / what-if analyses
- Static analysis of the system design
- Real-time simulations
- Showed that:
  - There were no dysfunctional interactions
  - Data was consistent (if SRs met)
  - Controllers (and Pilots) found the system useable

EUROCONTROL

Reaction to External Abnormalities – Arg1.4

- External failures included:
  - Landing aid (MLS/GBAS) or satellite interference or failure (GBAS).
  - Radio-communication Failure
  - Airfield-lighting outage
  - Radar-surveillance failure – loss of facility
- Mitigation in each case was Missed Approach (if no visual acquisition of runway)
- Other abnormalities considered:
  - Aircraft on-board emergencies
  - High crosswinds
- Risk was judged to be no higher than for current operations

EUROCONTROL

Arg1.5 – Mitigation of Internal Failures

EUROCONTROL

FHA/PSSA Main Conclusions

- ALC in LV introduces a new Hazard:
  - AC1 stops after Trigger Line, but before exiting OFZ, landing clearance having been given to AC2
- If AC2 lands (or goes around before 200ft agl) risk is negligible:
  - Trigger Line guarantees wing-tip clearance for landing case (SR!)
  - MA before 200ft agl would put AC2 above tail of AC1
- Worst case is if AC2 goes around later than 200ft agl:
  - Qualitatively, we feel that risk is probably small cf capacity benefits
  - Quantification of FHA/PSSA is in progress, to try to confirm this

EUROCONTROL

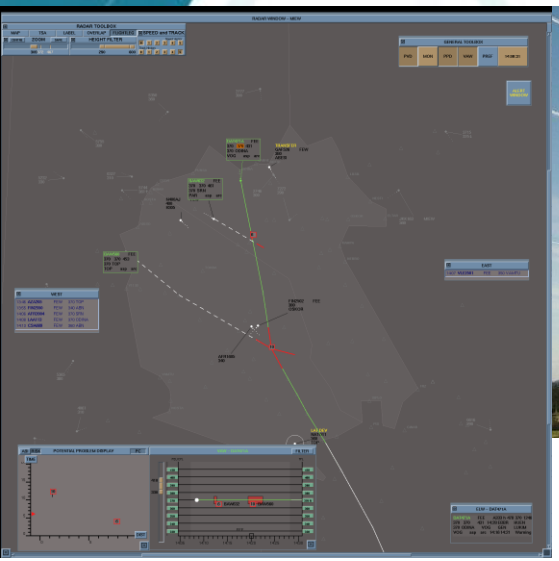
Lessons Learnt

- Original, failure-based safety assessment was too limited and unnecessarily complex
- New, broader approach:
  - is **more comprehensive** – addresses functional and performance issues relating to the Concept, not just reliability issues
  - has led to a **more rigorous** and detailed understanding and description of the ALC Concept and how it would have to be operated in practice
  - has produced a much **more readable** Preliminary Safety Case which starts with the basic idea and then gradually builds up the case

Around 30 Safety Requirements so far – most are FSRs !!

EUROCONTROL

Questions ??



?

EUROCONTROL

Safety Assessment Training Workshop

ACAS RA Downlink - Debrief

[Based on EUROCONTROL “ACAS RA Downlink Safety Summary Report”, Edition 1.2, 27 Mar 07, but restructured to fit the “Generic Safety Argument]

Derek FOWLER
JDF Consultancy LLP

February 2008

EUROCONTROL

Safety Criteria

- The risk of an accident shall be:
  - Substantially less than currently exists from ACAS-ATC interaction
  - reduced as far as reasonably practicable

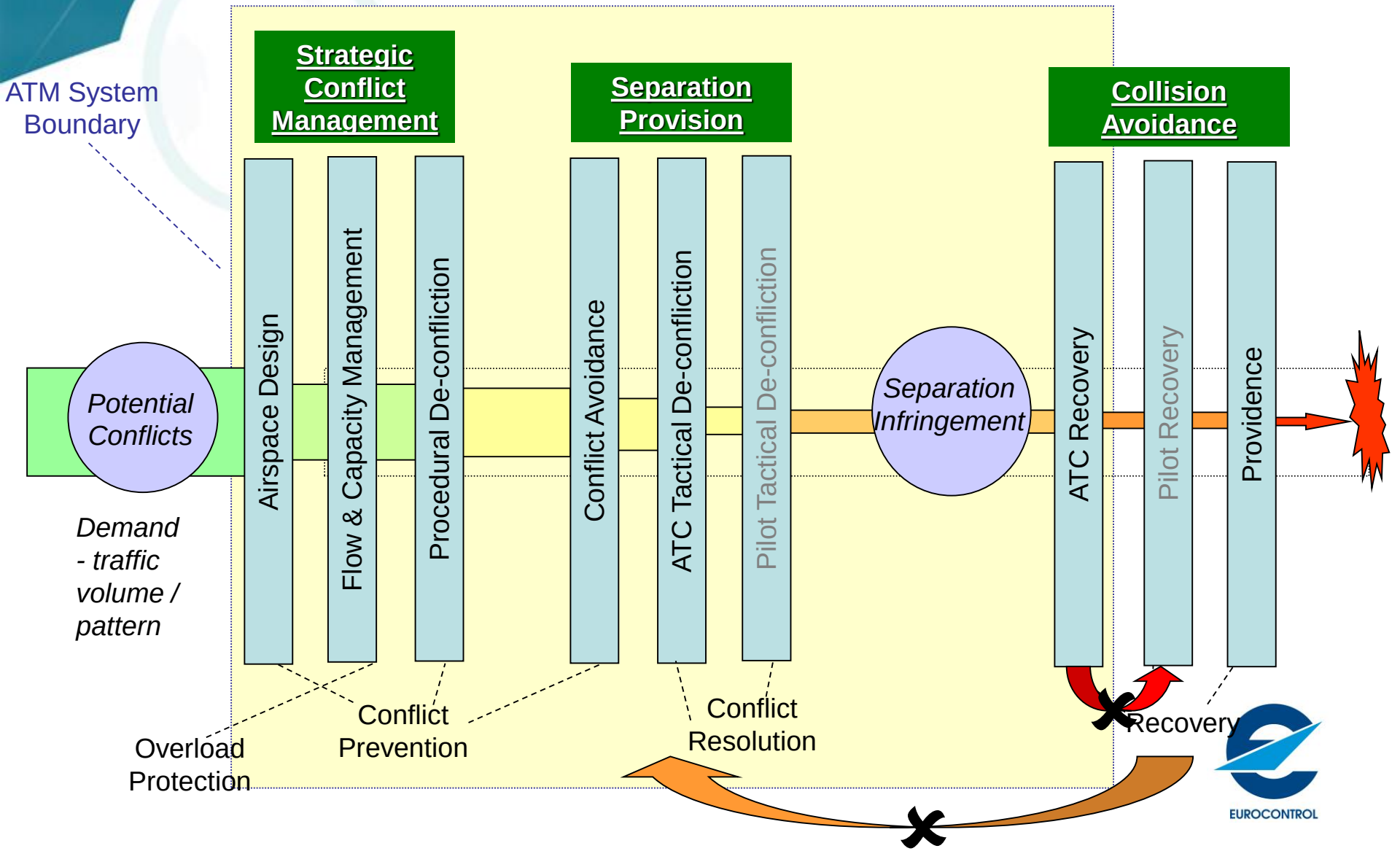
EUROCONTROL

Arg1.1 – Intrinsic Safety

The potential to satisfy the Safety Criteria

EUROCONTROL

A "Barrier Model" View



Session 3 !!

Pre-existing Hazards

Benchmark for Success Approach

- Two aircraft encounter a genuine RA
- Multiple aircraft encounter a genuine RA
- Aircraft encounters an ‘unnecessary’ RA
- Aircraft encounters a false RA
- Aircraft does not react to an RA

EUROCONTROL

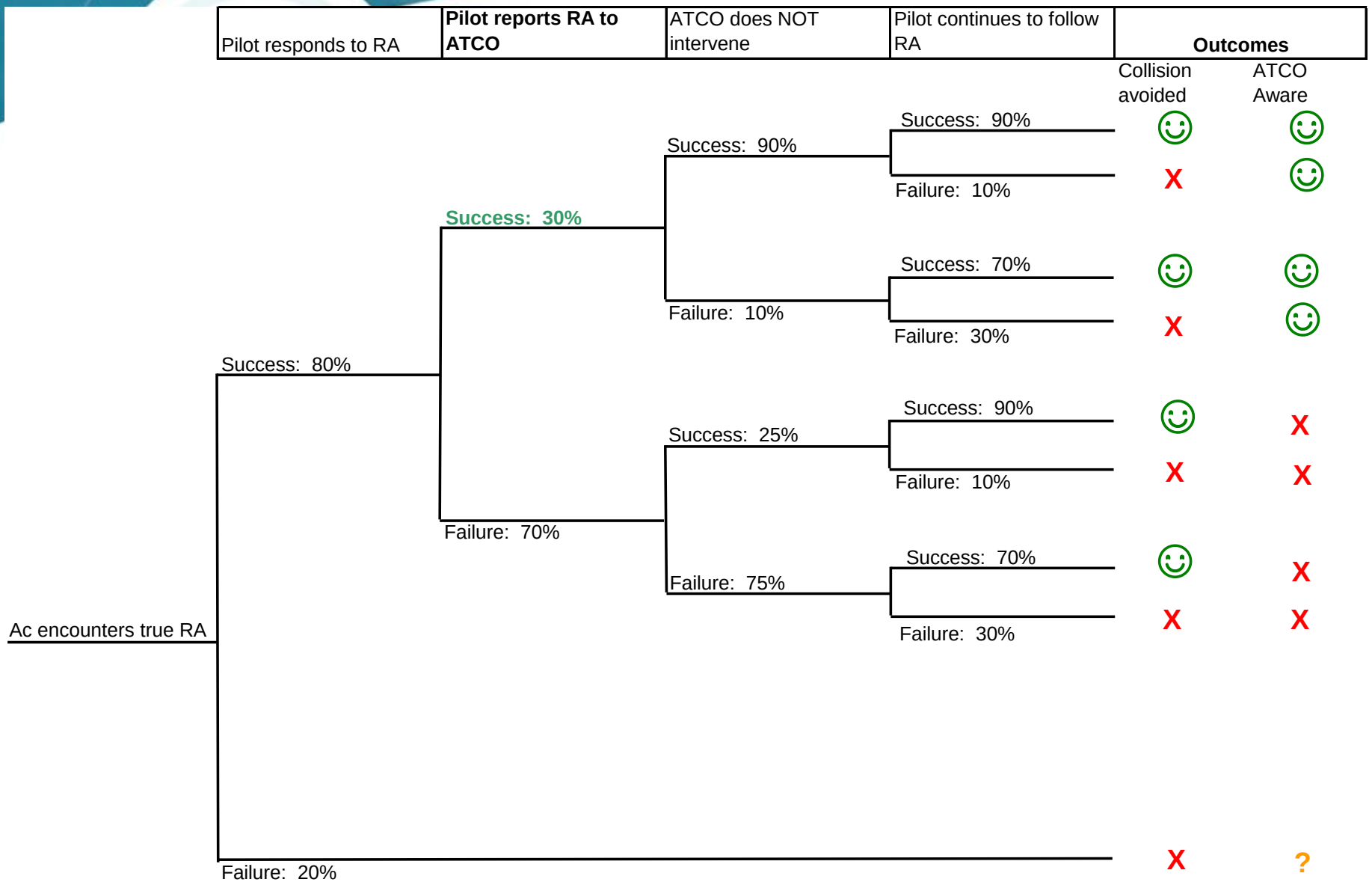
Pre-RA Downlink Deficiencies

- System is designed to mitigate hazards BUT much less effective if:
  - Pilot voice report of RA is incorrect, missing or late:
    - 85% of RAS typically reported within 30 secs
    - 15% never reported
  - Threat aircraft is not identified
  - Controller attempts to issue clearance / instruction
  - Pilot does not ignore Controller clearance / instruction
  - Frequency is blocked
  - RT interchange is protracted due to confusion
  - Clear of Conflict report is missing or late

Modelled as an Event Tree….>>>

EUROCONTROL

Pre-FARADS Event Tree - Illustrative



Safety Potential

- RA Downlink has potential to improve safety because:
  - Reduced “uninformed ATC intervention” in high-risk RAs, by 80-90%
  - Improved Controller situational awareness
- Key functionality / parameters :
  - Display of RA / direction: throughout RA - removed on RA completion
  - RA to be displayed in <10 secs after activation in cockpit
- Reduction in collision risk lessened if there is a high probability of pilots ignoring ATC intervention

EUROCONTROL conducting study into effects of STCA on situation !

EUROCONTROL

Arg1.2 – Design Completeness

Specification of Functional Safety Requirements

EUROCONTROL

Examples of Initial (Functional) Safety Requirements

- RAs shall be **downlinked** and displayed to the Controller
- **Downlinked** RA shall be displayed to the Controller within 10 seconds of the RA being activated in the Cockpit
- The RA Downlink **display** shall remain active until the aircraft is 'Clear of Conflict'
- RA Downlink **display** shall show the direction of the RA, as displayed by TCAS to the Pilot
- RA Downlink **display** shall identify the subject aircraft and intruder aircraft …
- Training shall reinforce that **Controllers** shall not issue clearances to aircraft involved in an RA
- **Pilot** training shall reinforce the requirement to report RAs that require a deviation from clearance as soon as is practical / possible.

EUROCONTROL

Techniques for Arg1.3 – Design Correctness

- Scenario / what-if analyses
- Real-time simulations

EUROCONTROL

Scenarios / What-ifs

- Non-equipped aircraft
- Possible misinterpretation of RA Downlink symbols
- Screen blocking caused by the RA Downlink tags
- RA Downlink data sharing between adjacent ATC Units
- Non-universal implementation of RA Downlink
- Responsibility for separation will be ambiguous at the end of the event if there is no ‘Clear of Conflict’ report from the flight crew
- Cannot distinguish between RAs that do / don’t require deviation from clearance
- Two methods for reporting RAs - ie voice and RA Downlink.
- RA Downlink might distract the Controller
- Controllers might be exposed to an excess of information on the screen
- The provision of traffic information during an RA could lead to wrong visual acquisition of threat aircraft

Examples of Additional FSRs

- Where a non-ACAS equipped aircraft is involved in an RA event, the Mode S address (where downlinked by the ACAS II-equipped aircraft) shall be **displayed** to the Controller
- Once an RA is displayed to the **Controller** via RA Downlink they shall not attempt to issue clearances to any aircraft involved in the event until either:
  - the display is cleared from the radar screen and the Pilot has reported ‘Clear of Conflict’ or;
  - the RA has been cleared from the radar display for a minimum of 20 seconds and it is clear that the aircraft involved are diverging
- An RA Downlink **data-sharing network** shall be implemented between all RA Downlink enabled ATC centres
- There shall be no change in procedures imposed on **Flight Crews** with respect to actions during or immediately after an RA encounter

Total of 12 additional FSRs

Simulation Findings

- Controller's intervention in an RA event:
  - Timely and reliable RA Downlink could prevent the Controller from issuing clearances to aircraft experiencing an RA
- Controller's Situational Awareness
  - RA Downlink can benefit both speed & accuracy of locating aircraft on screen
  - RA Downlink enables Controller to anticipate RA and Clear of Conflict reports
  - Improved ATC general situational awareness, facilitating the prevention of further RAs with aircraft that currently are not involved
  - Intruder identified in majority of cases
  - RA visible for the duration of the event

EUROCONTROL

Reaction to External Abnormalities – Arg1.4

- Scenarios included:
  - Pilot does not comply with RA indication in cockpit
  - 'Unnecessary' RAs - eg excessive vertical speed of aircraft
  - False RA generated in aircraft
- Additional Functional Safety Requirements include:
  - ATC **Procedures** shall make it clear to Controllers what they should do in the event of an aircraft manoeuvring in a manner different to that displayed by RA Downlink
  - **Flight Crew operating procedures** and training shall require Pilots to reduce their rate of climb / descent to less than 1500ft/min when in RVSM airspace or within the last 1000ft before cleared level
  - Procedures shall make it clear to Controllers what they should do if an RA is displayed for an aircraft when there does not appear to be an intruder present…

EUROCONTROL

Arg1.5 – Mitigation of Internal Failures

- Scenarios include:
  - Loss of RA Downlink
  - False indication of RA
  - Spurious, multiple RAs
- Mitigations include:
  - RA Downlink shall have operational availability of at least 95%
  - The frequency of a false display of an RA to the Controller (ie an RA that does not exist, or annotation of an RA to the wrong aircraft) shall not exceed 10^{-5} per operating hour
  - Controllers shall have the ability to disable RA Downlink for selected aircraft / all aircraft

EUROCONTROL

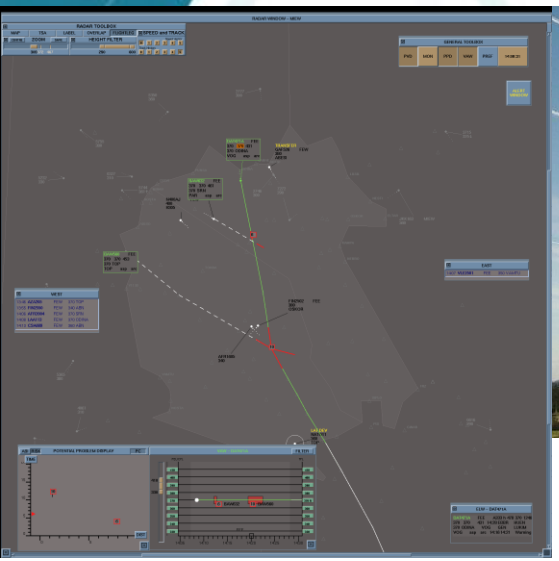
Safety Case Conclusions

- RA Downlink will improve Controller situational awareness and prevent some inadvertent ATC intervention during an RA, although there are inherent safety issues
- From the evidence gathered there is a net positive benefit of RA Downlink if all of the proposed Safety Requirements can be satisfied
- However, whether the benefit is substantial is subjective. It should be determined whether the costs of achieving the Safety Requirements are justified by the benefits of RA Downlink, taking into consideration the possible disadvantages
- The are some ambiguities / inconsistencies in and between PANS-OPS and PANS-ATM regarding current responsibilities during an RA

"The jury is still out" !!

EUROCONTROL

Questions ??



?

EUROCONTROL