versität Bielefeld
hnische Fakultät

R|V|S
Rechnernetze und
Verteilte Systeme

ACAS and the July 1 Midair

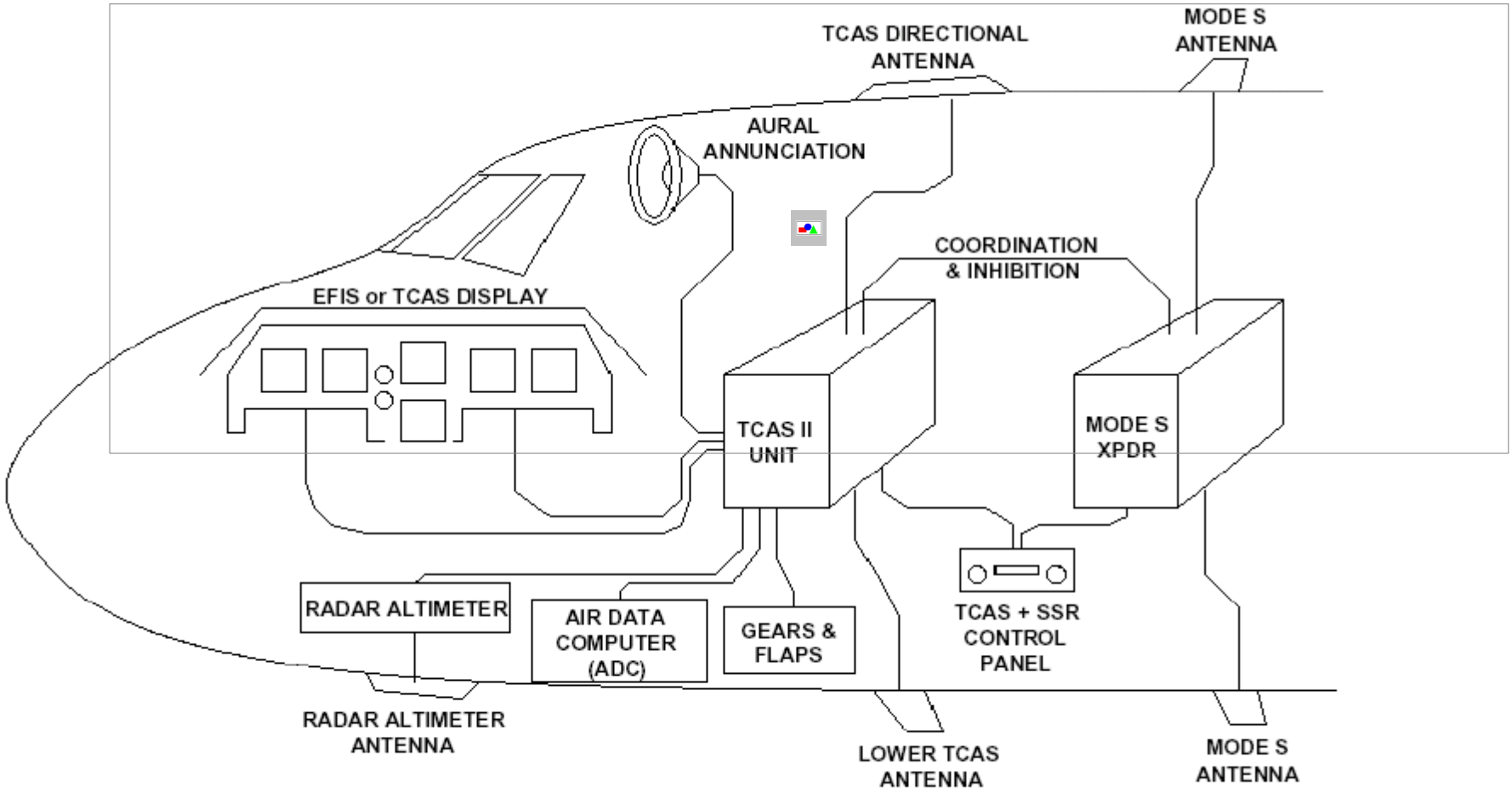
The Systems and Their Properties

Peter B. Ladkin
ladkin@rvs.uni−bielefeld.de

The Technology − ACAS

- ACAS − Airborne Collision Avoidance System
- Current version ACAS II, required in EUR−AS since Jan 2000 − Mar 2001 (transition period)
- Only provider: Honeywell, with TCAS II
  - V6.04a in use: not ACAS II−compliant
  - V7 available since late 2000
- TCAS warns of other aircraft in the immediate vicinity (Traffic Advisory, TA)
- TCAS advises an avoidance manoeuvre (Resolution Advisory, RA) if "intruder" close

The Technology – TCAS



- From Eurocontrol's ACAS II Training Manual

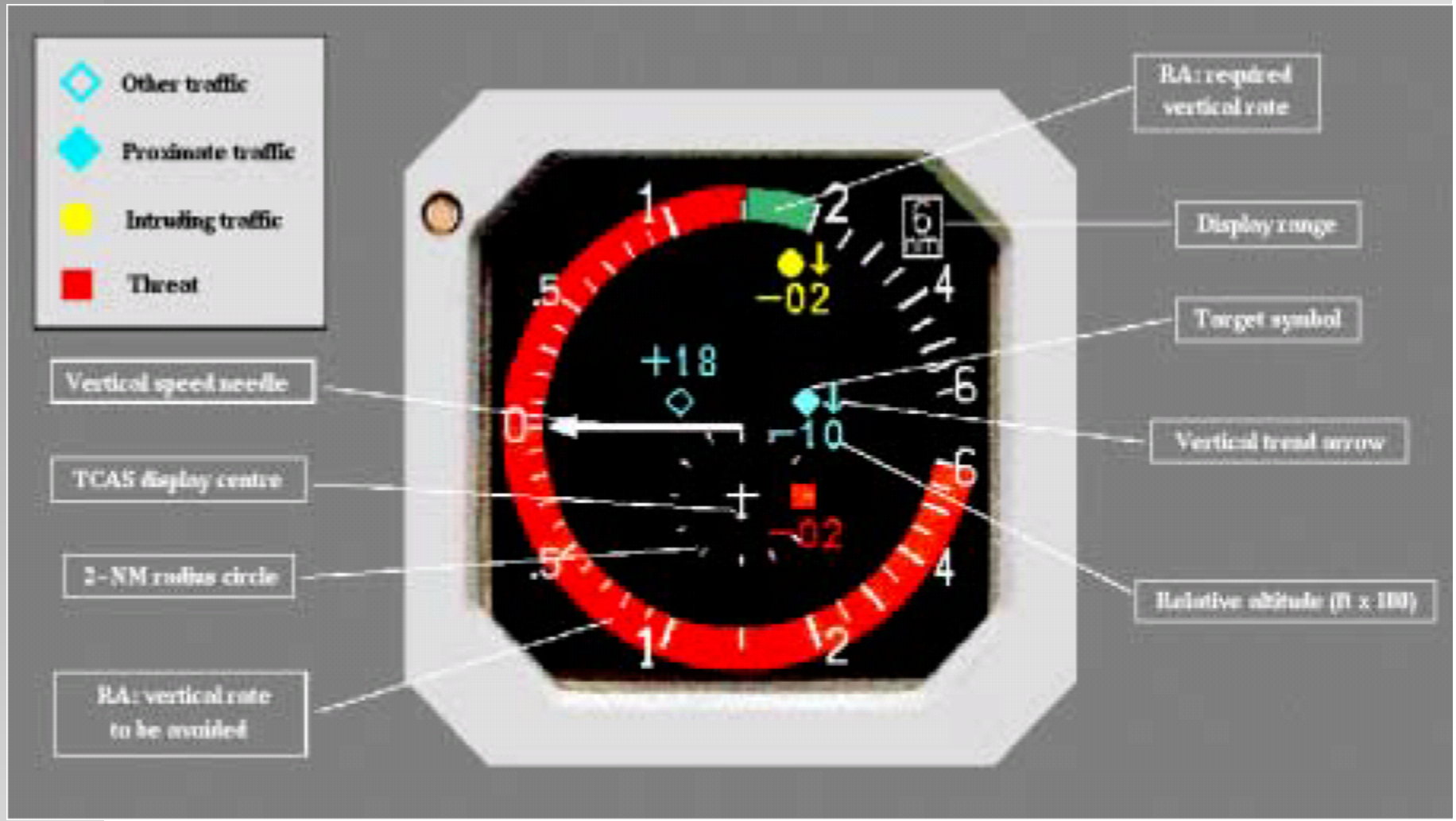
  www.eurocontrol.int –> Projects –> ACAS –> Training Materials –> Manual Vers. 2

The Technology – ACAS

- There is a screen which provides a "bird's eye" view, and highlights the position of "intruders"
- Positional information is only approximate
- Advisories are visual (highlighted screen) and aural (synthesised voice)

- Two levels of advisory:
  - Traffic Advisory (TA). Vigilance expected from crew
  - Resolution Advisory (RA). Manoeuvre expected

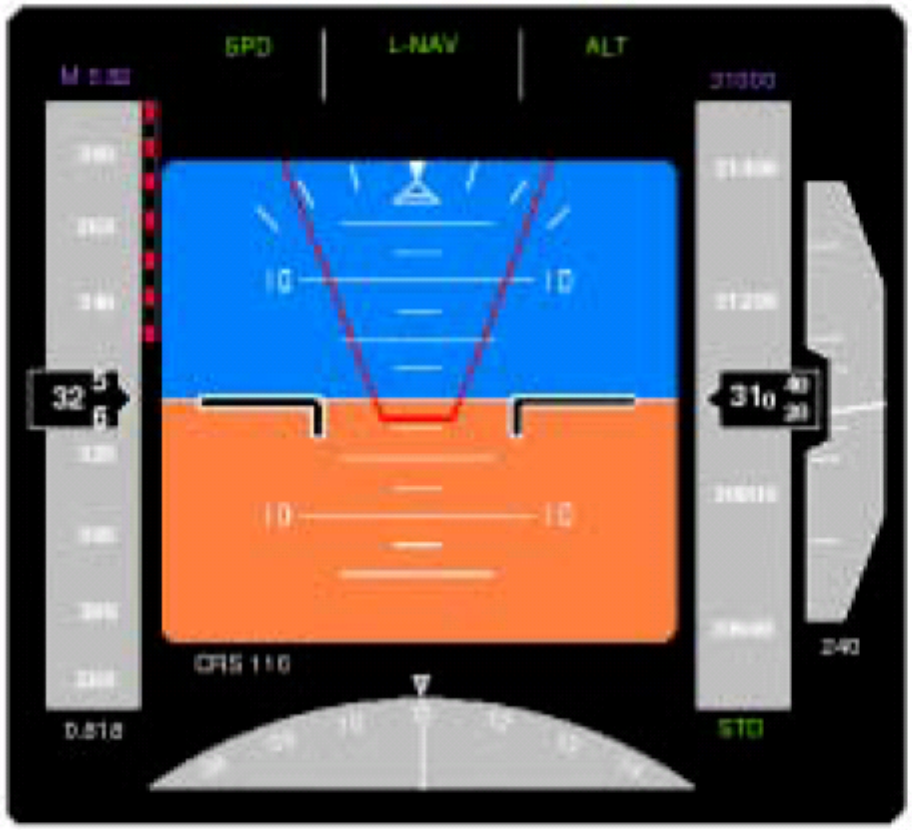
TCAS "Classical" Display



- From Eurocontrol's ACAS II Training Manual

  www.eurocontrol.int −> Projects −> ACAS −> Training Materials −> Manual Vers. 2

TCAS Display in "Glass" Cockpits



RA on the artificial horizon

RA on the Vertical Speed Indicator (VSI)

- From Eurocontrol's ACAS II Training Manual

  www.eurocontrol.int –> Projects –> ACAS –> Training Materials –> Manual Vers. 2

TCAS Display in "Glass" Cockpits

- From Eurocontrol's ACAS II Training Manual

  www.eurocontrol.int –> Projects –> ACAS –> Training Materials –> Manual Vers. 2

The Technology – ACAS RA

- RAs are vertical–sense only ("Climb", "Descend")
- RA issued within an "alert threshold" based on predicted "time to go" (ttg) before collision
- Two–level ("climb", "increase climb") based on 1,500 fpm, resp. 2,500 fpm vertical speed
- Iterative (two consecutive RAs may be issued)
  - strengthening: "climb", "increase climb"
  - constant:: "climb", "maintain vertical speed"
  - weakening: "climb", "adjust vertical speed"
  - reversing: "climb", "descend NOW"

TCAS RA on the IVSI (Eurocontrol T.M.)

Descend

Climb

Adjust vertical speed
(weakening advisory)

Increase climb
(strengthening advisory)

Maintain vertical speed
(maintain climb)

Adjust vertical speed
(reduce rate of descent)

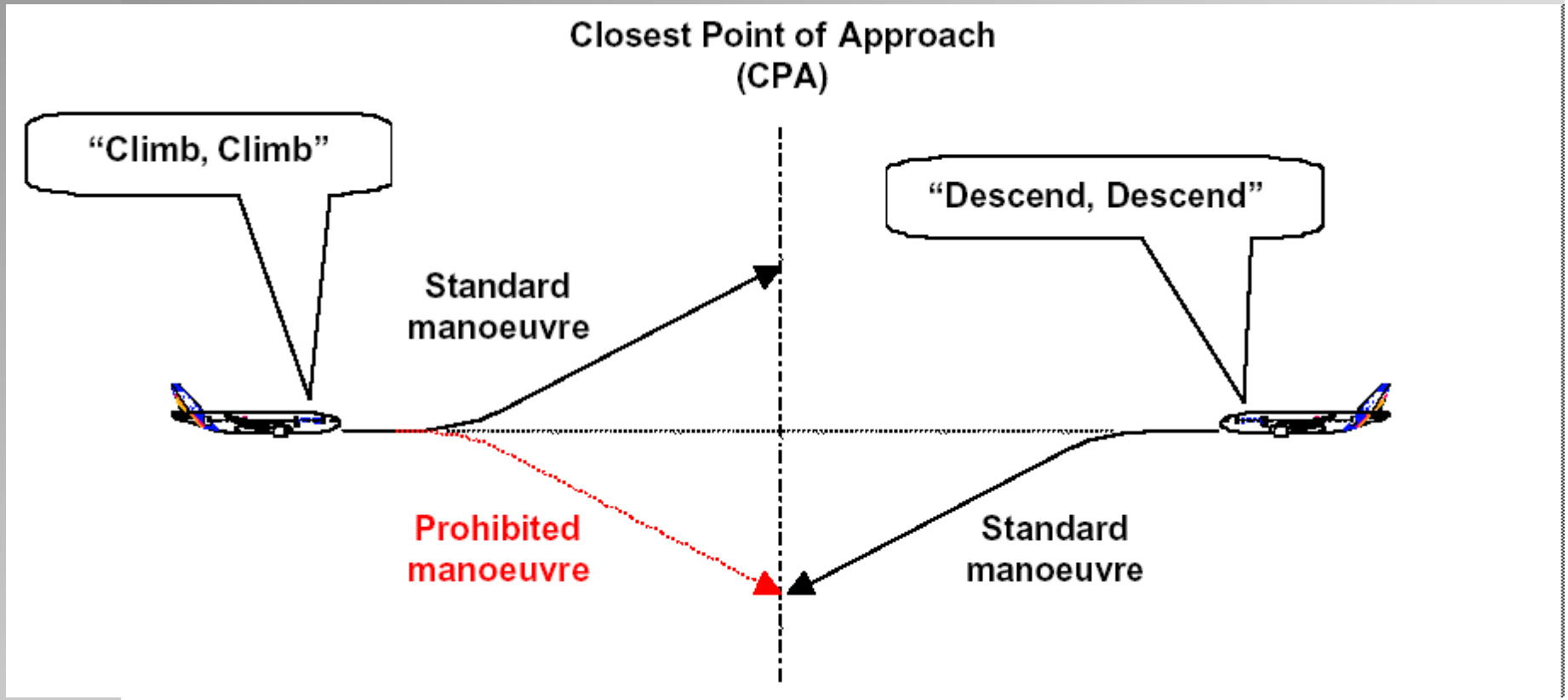
Adjust vertical speed
(multi-threat advisory)

Monitor vertical speed

The Technology – ACAS RA

- "Protected volume" is a vertically–truncated sphere (essentially a vertical cylinder) with
  - radius = (relative speed) x ttg
  - Length = 600–800 vertical feet (low closure rate) or
  - Length = (relative vertical speed) x ttg (high closure rate)
- Avoidance manoeuvres negotiated between aircraft
  - One receives "climb" RA, the other "descend" RA
- RAs normally conform to altitude differences
  - The higher aircraft receives a "climb" RA, the lower "adjust vertical speed" or "descend"
- –– but must not: so–called "crossing RAs"
  - "climb, crossing climb"

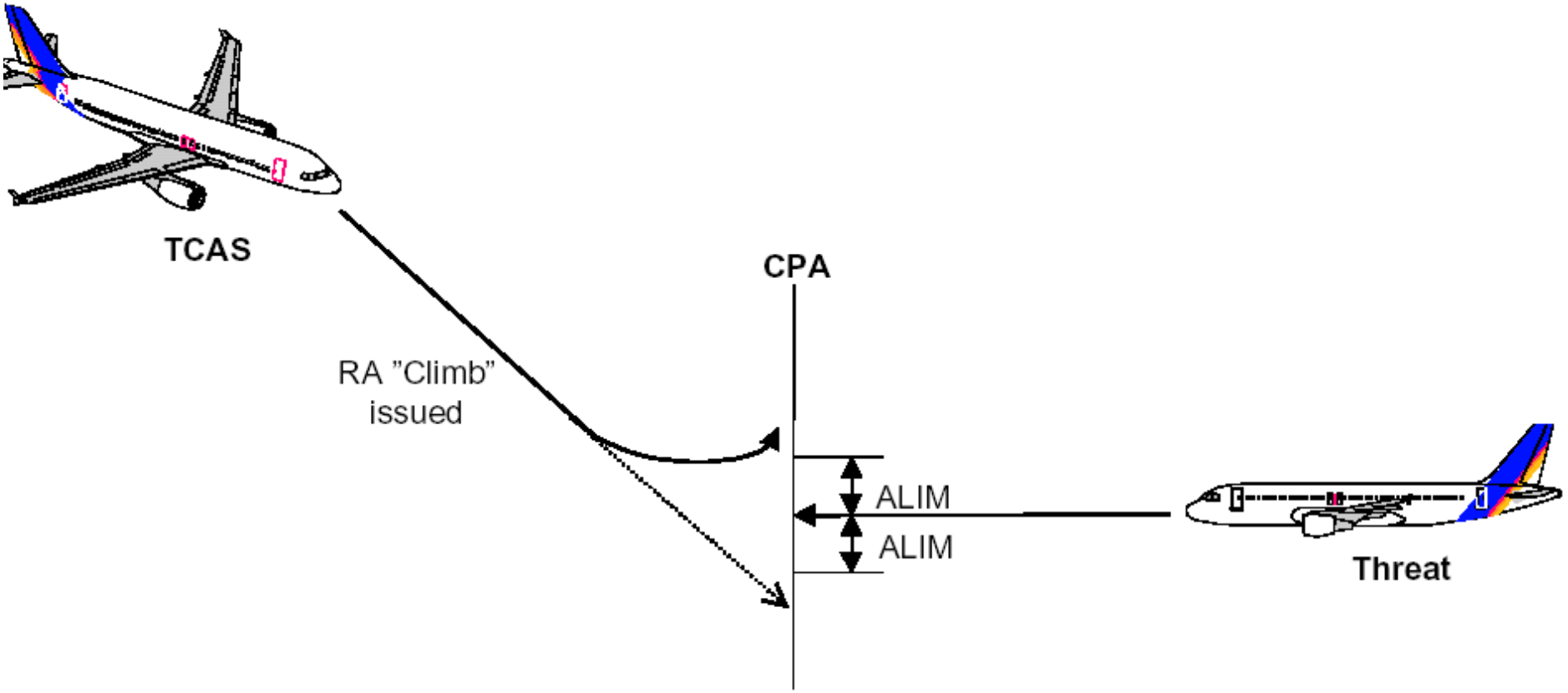
Standard Manoeuvre



- From Eurocontrol's ACAS II Training Manual

  www.eurocontrol.int −> Projects −> ACAS −> Training Materials −> Manual Vers. 2

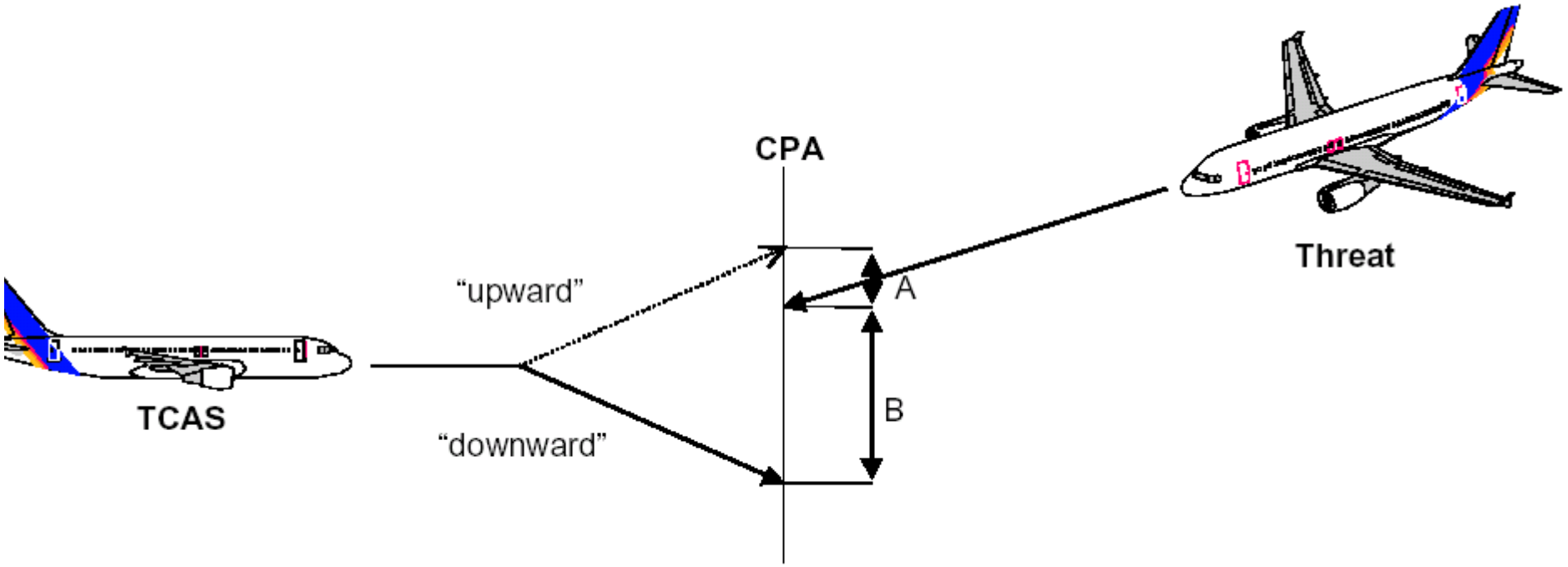
Non−crossing RA



- From Eurocontrol's ACAS II Training Manual

  www.eurocontrol.int −> Projects −> ACAS −> Training Materials −> Manual Vers. 2

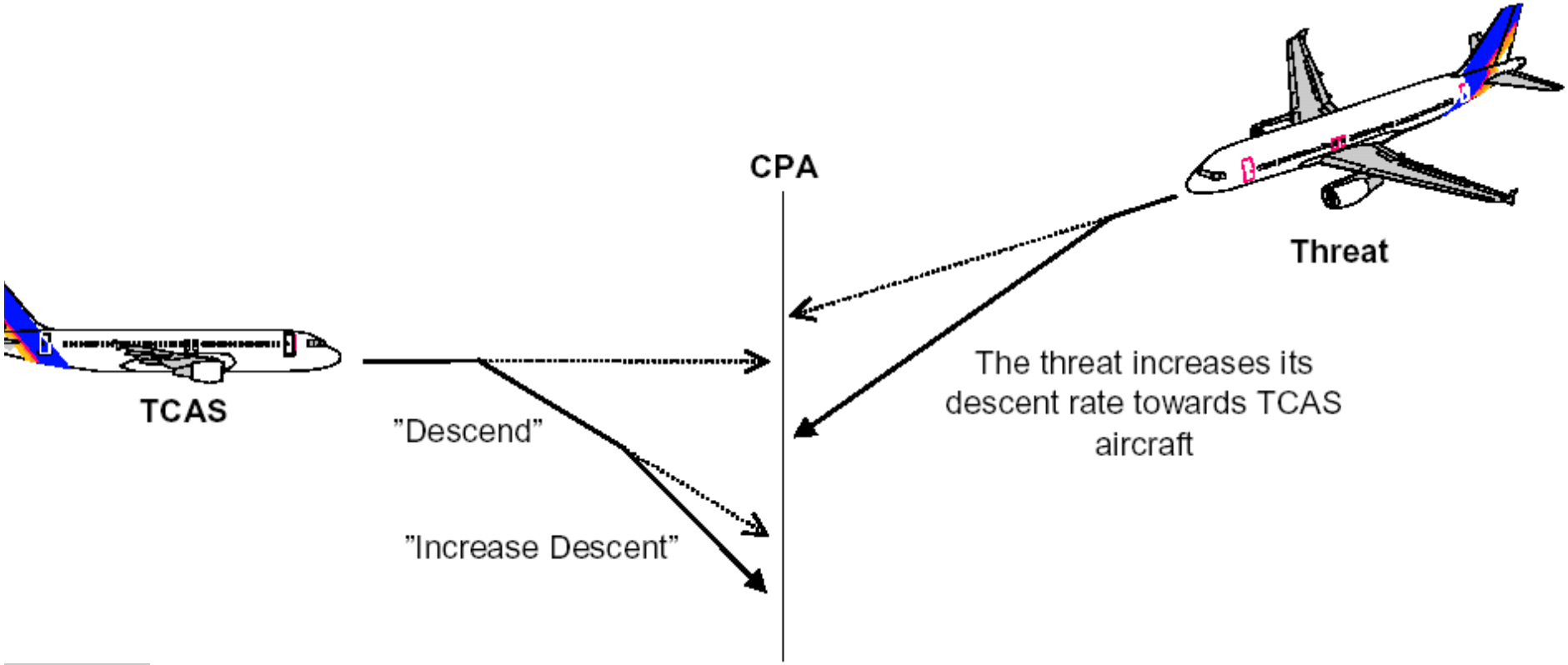
RA Sense Selection



- From Eurocontrol's ACAS II Training Manual

  www.eurocontrol.int −> Projects −> ACAS −> Training Materials −> Manual Vers. 2

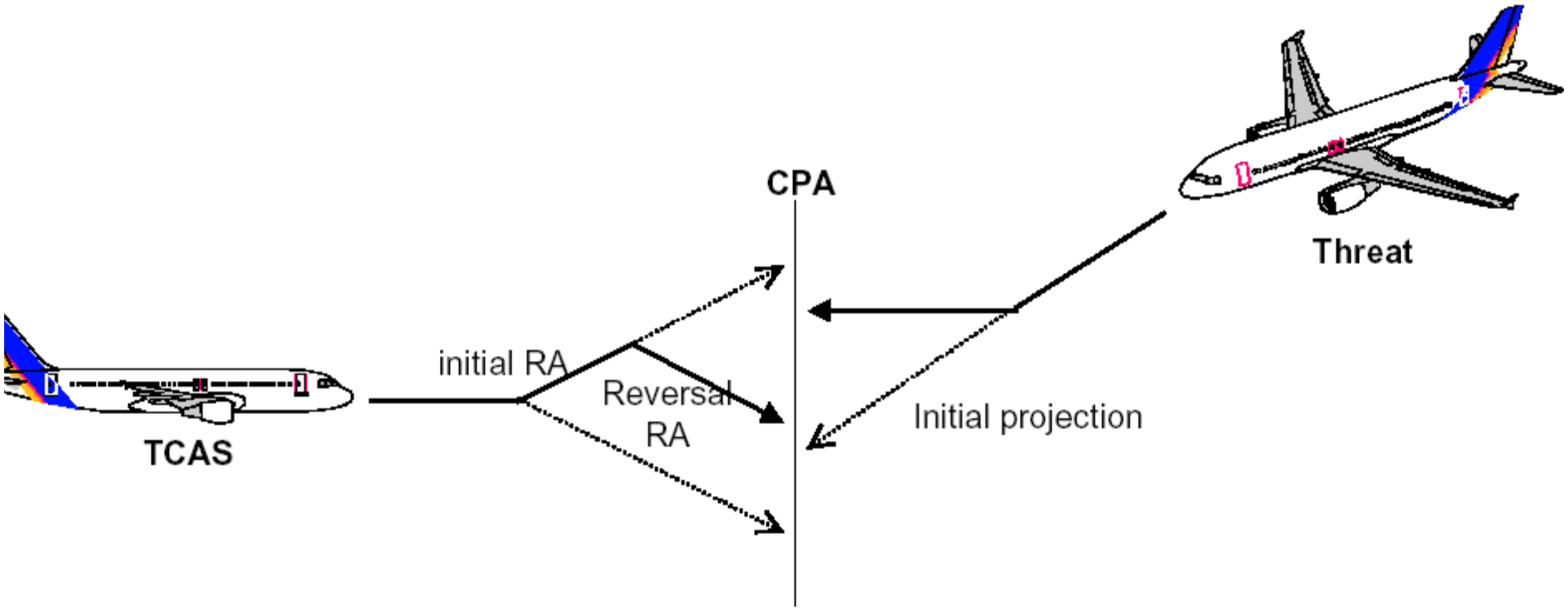
TCAS Iterated Resolution Advisory



- From Eurocontrol's ACAS II Training Manual

  www.eurocontrol.int −> Projects −> ACAS −> Training Materials −> Manual Vers. 2

TCAS Iterated Resolution Advisory



- From Eurocontrol's ACAS II Training Manual

  www.eurocontrol.int −> Projects −> ACAS −> Training Materials −> Manual Vers. 2

ATC Function

- Aircraft at FL 290 − FL 410 are under "positive control"
  - That is, airspace is "cleared" for them by ATC, which guarantees that no other aircraft will be in the cleared airspace
  - Clearances are both long−range (at start) and dynamic (aircraft entering a controller’s range will be given modified clearances to avoid other aircraft already under hisher control)

The Problem

- ATC clears airspace
- Following an ACAS RA, an aircraft departs from cleared airspace
- The airspace into which the manouevring aircraft enter may not be clear for them
  - Hence: following RAs may induce further risk of collision, hence further RAs with other traffic
  - One hopes such "chain reactions" will not happen
- The vertical volume of cleared airspace under RVSM is half what it used to be

Lake Constance Midair

- 1 July, 2002 over Lake Constance, S Germany
  - AC under control of Zürich ATC
    - Same controller, same frequency
  - DHL 611 northbound, in contact for 13+ minutes
  - BTC 2937 westbound, in contact for 4+ minutes
  - Both at FL 360 initially

Lake Constance Midair

- TCAS TA received by both aircraft
- 7 seconds later, BTC received ATC advisory to descend "expedite" for traffic
- 7 seconds later, BTC follows it. At the same time, DHL receives "descend" RA and BTC a "climb" RA
- 7 seconds later, ATC repeats descent advisory, advises of traffic at "2 o’clock". DHL is at 10 o’clock

Lake Constance Midair

- 7 seconds later, DHL receives strengthened RA "increase descent"
- 9 seconds later, DHL advises ATC of TCAS descent
- 5 seconds later BTC receives strengthened RA "increase climb" (14 seconds after DHL's 2nd RA!)
- 6 seconds later, they collide

Observations

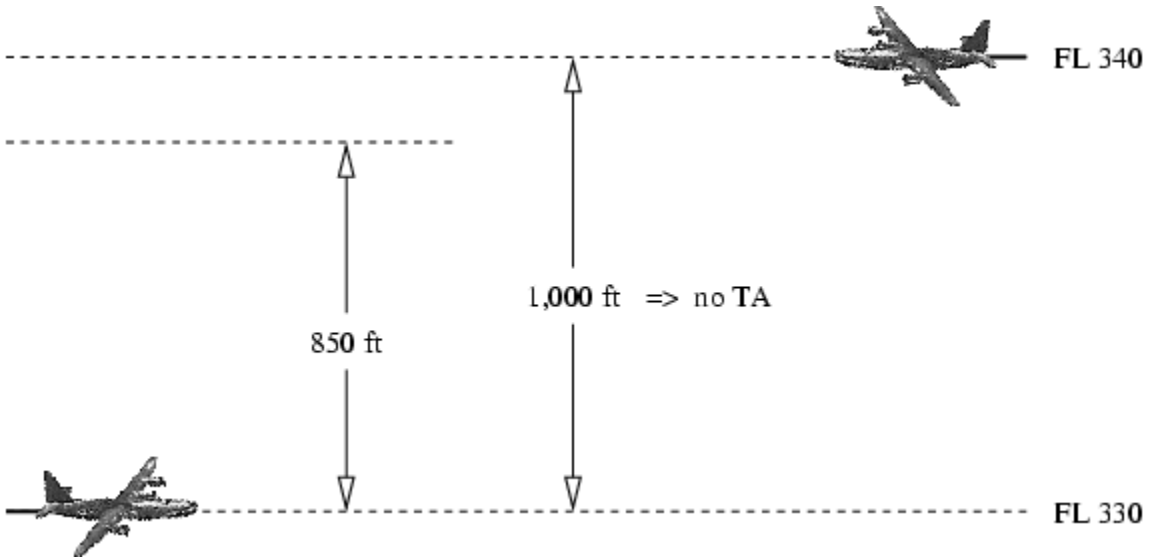
- ACAS use was a causal factor in the accident chain, by the Counterfactual Test
  - DHL and BTC collided "at about FL 350"
  - Had DHL not descended, BTC and DHL would not have collided
  - DHL would not have descended, had ACAS avionics not been installed or had the RA not been followed by DHL's CRW
- Note I say "ACAS use" and not − yet − the "ACAS system"

ACAS with RVSM

- There are interactions
  - Interaction not only through valid RAs (Constance)
  - But also interaction through spurious RAs (TRA, turbulence, oscillations, allowed system error)

- Risk can be increased by RAs
  - Interaction through spurious RAs can increase risk over that without ACAS (TRA)
  - So can multi−aircraft interaction triggered by a valid RA, if it sets forth a chain reaction

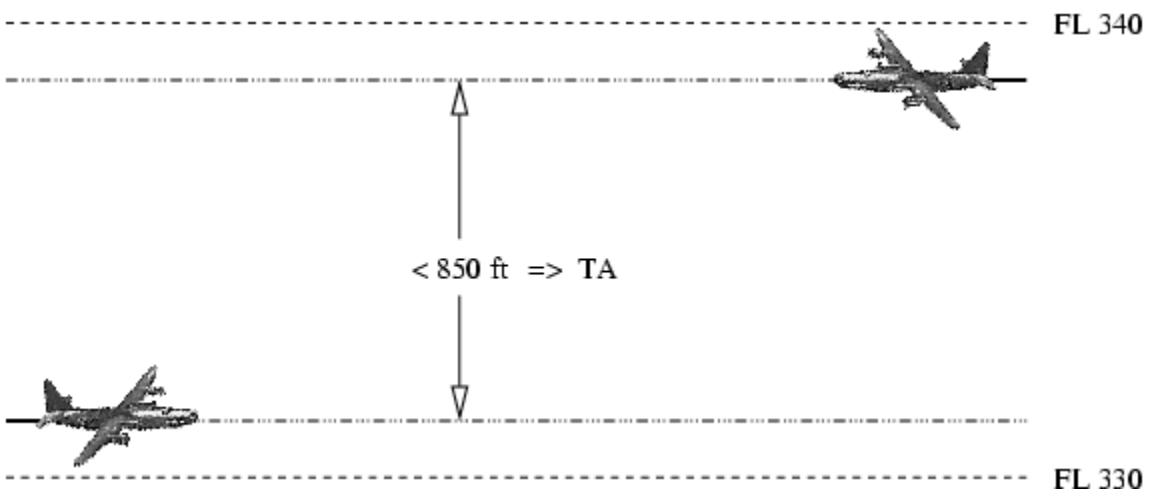
ACAS in RVSM. The Standard Case



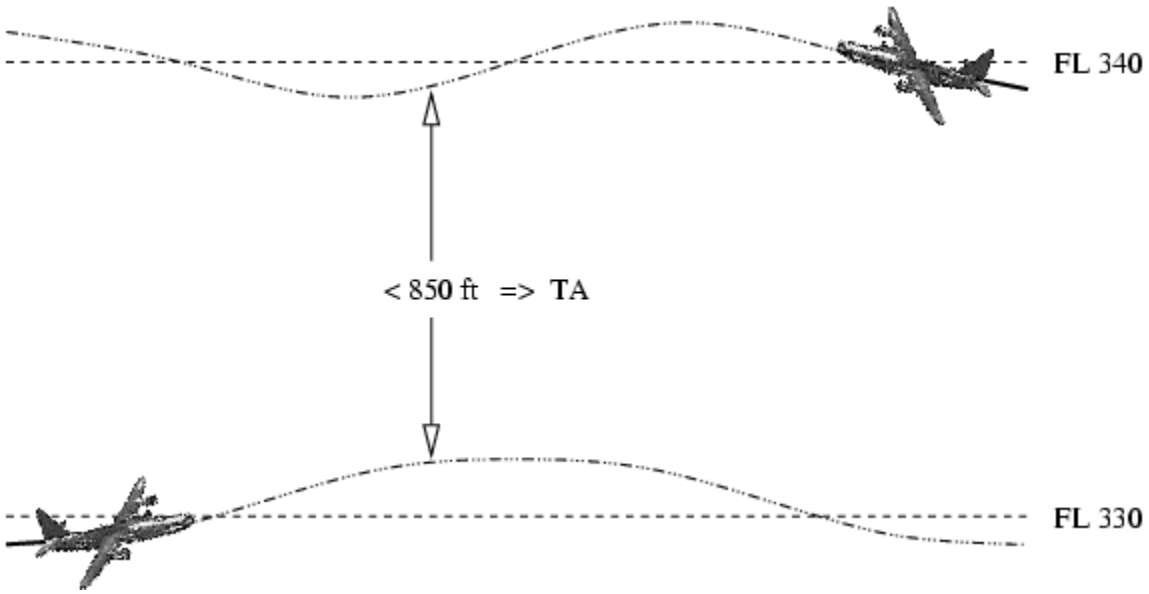
Spurious RA in RVSM: Allowed Errors

- Maximum allowed FL offset 65 ft
- Altitude report ing in 100−ft increments (can also be 25-ft increments)
- Aircraft can "see" each other at < 850 ft separation
  - Aircraft A at FL 340 but 51 ft low
  - Aircraft A reports at FL 339 (100−ft increment)
  - Aircraft B TCAS "sees" AC A at FL 339
  - Aircraft B at FL 330 but 51 ft high
  - TCAS calculates relative altitude 849 ft
  - TA is generated

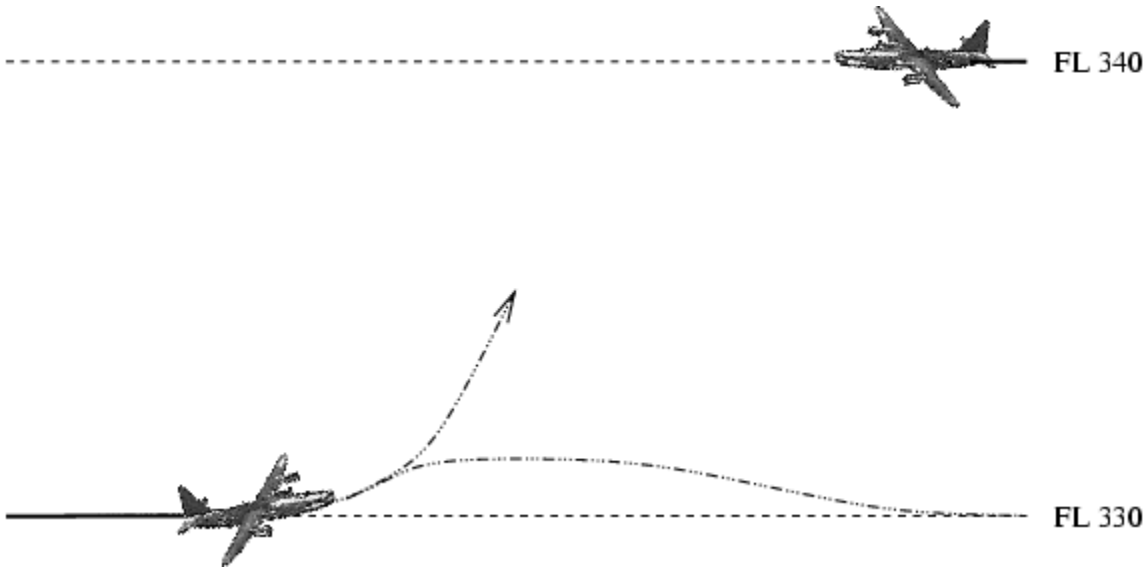
Spurious RA in RVSM. Allowed Errors



Spurious RA in RVSM. Oscillation



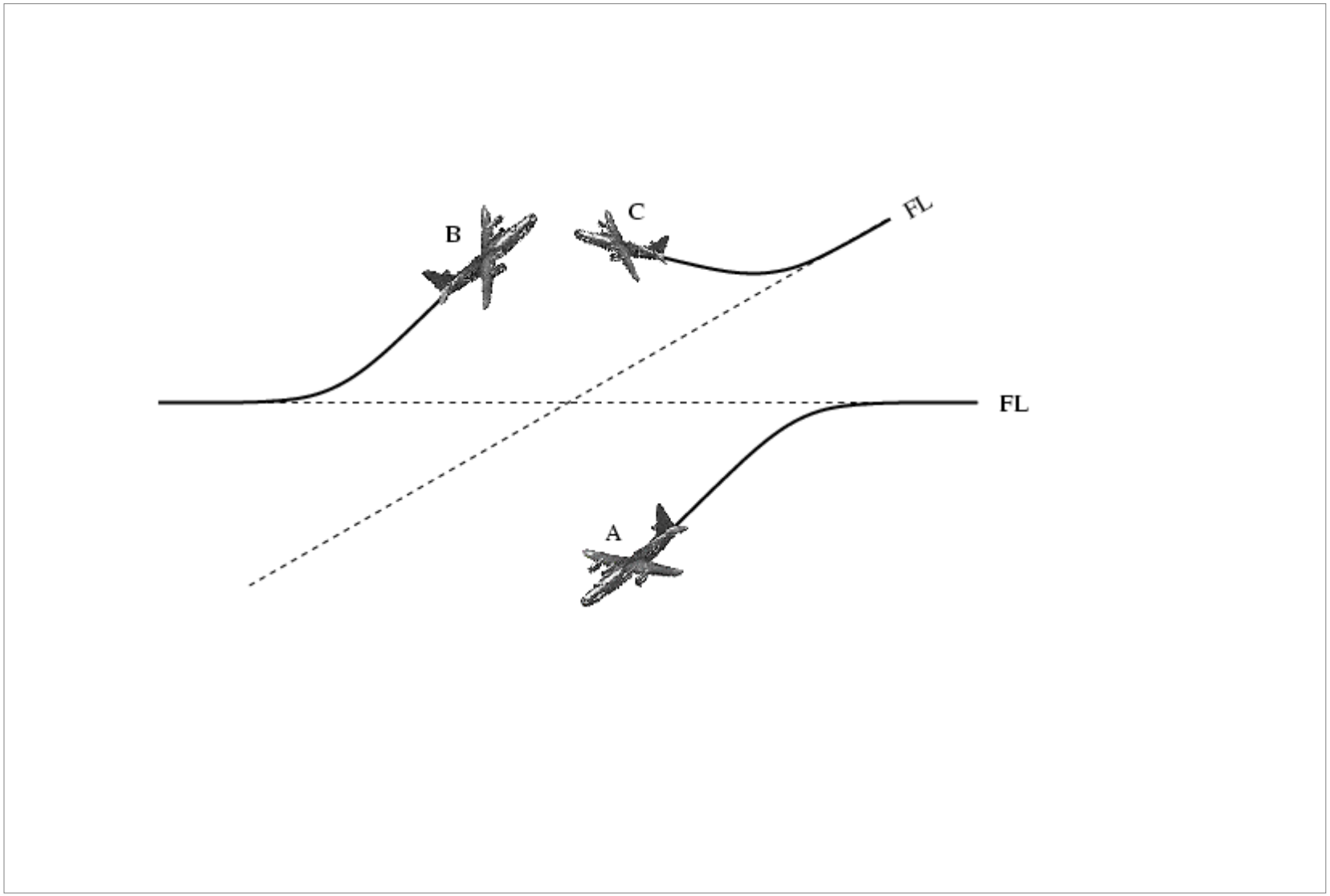
Spurious RA in RVSM. Turbulence



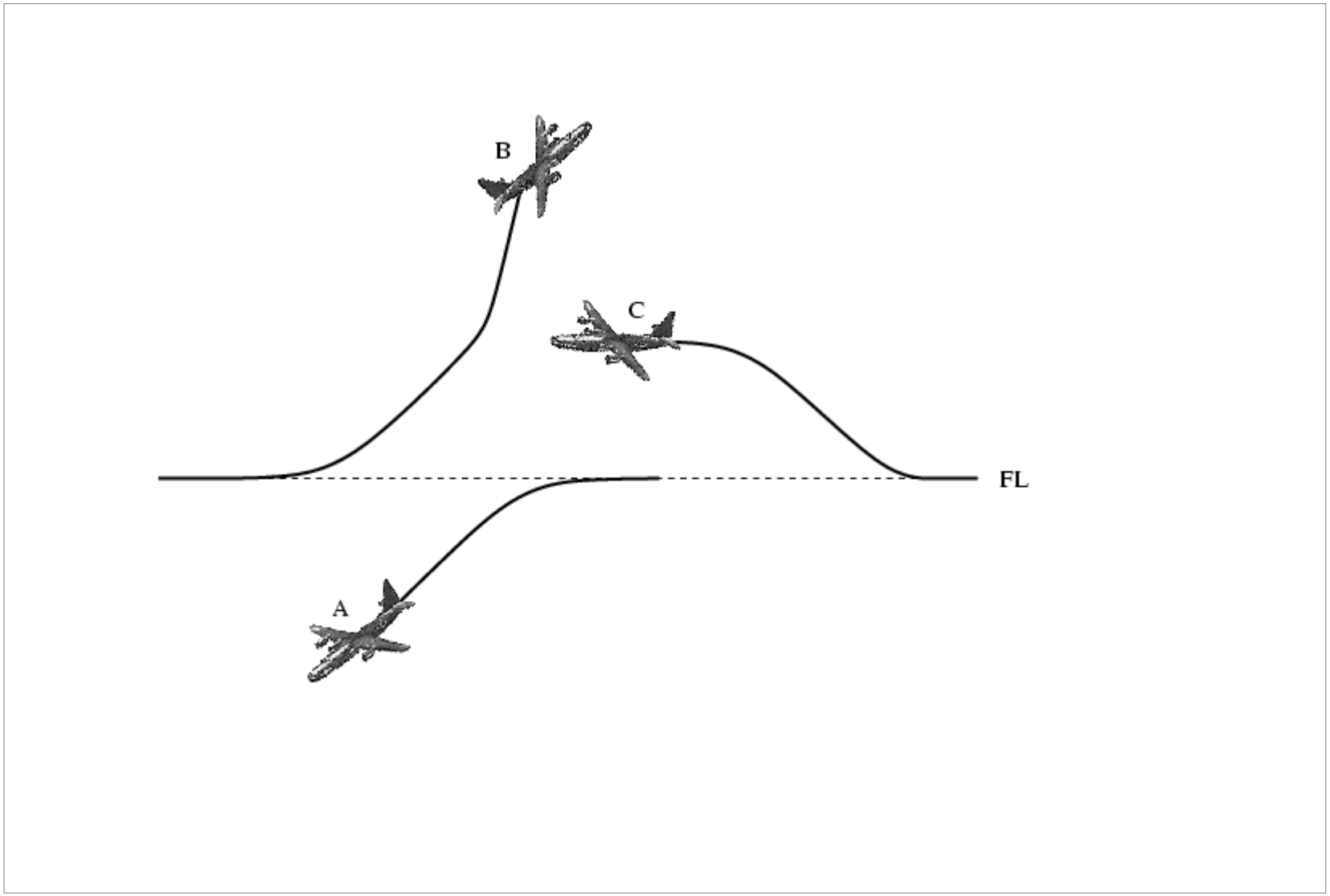
ACAS Safety

- Eurocontrol ACAS II Training Manual:
  - "TCAS is able to handle multi−threat situations either by attempting to resolve the situation with a single RA, which will maintain safe vertical distance from each of the threat aircraft, or by selecting an RA that is a composite of non−contradictory climb and descend restrictions."
  - "TCAS significantly improves flight safety. However, it cannot entirely eliminate all risks of collision. Additionally, as in any predictive system, it might itself induce a risk of collision"

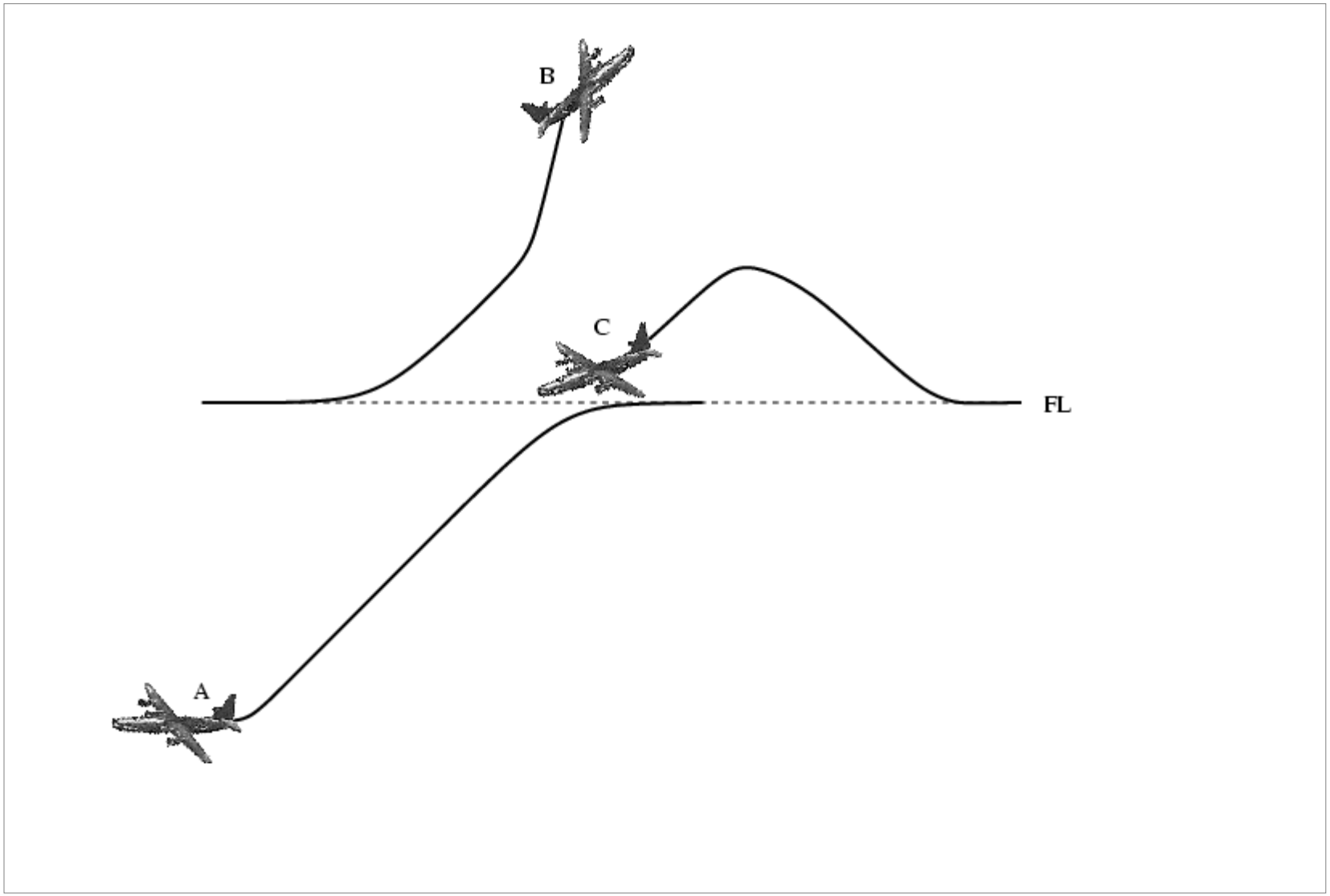
Three−Aircraft Conflict: Situation 1



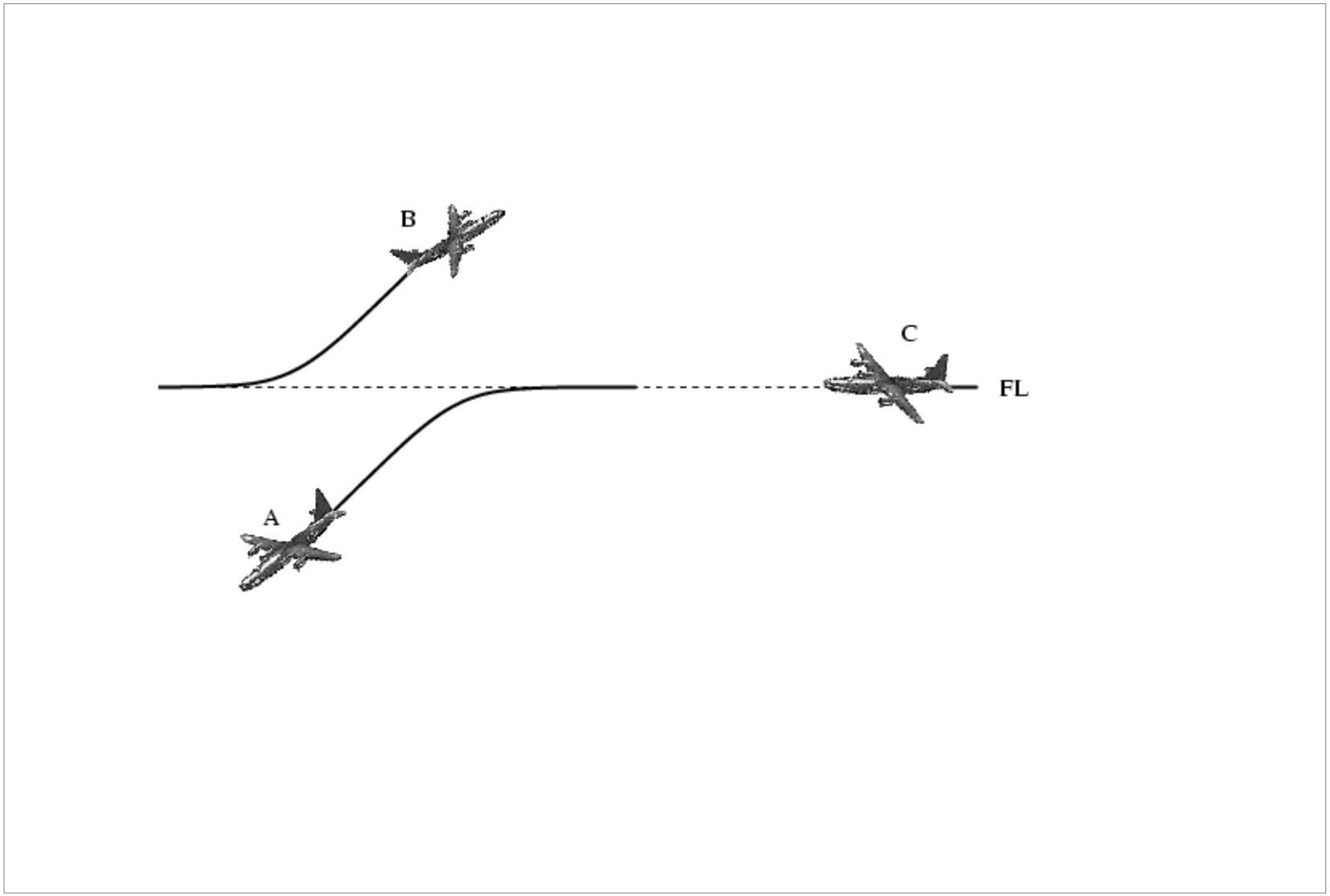
Situation 1: Resolution



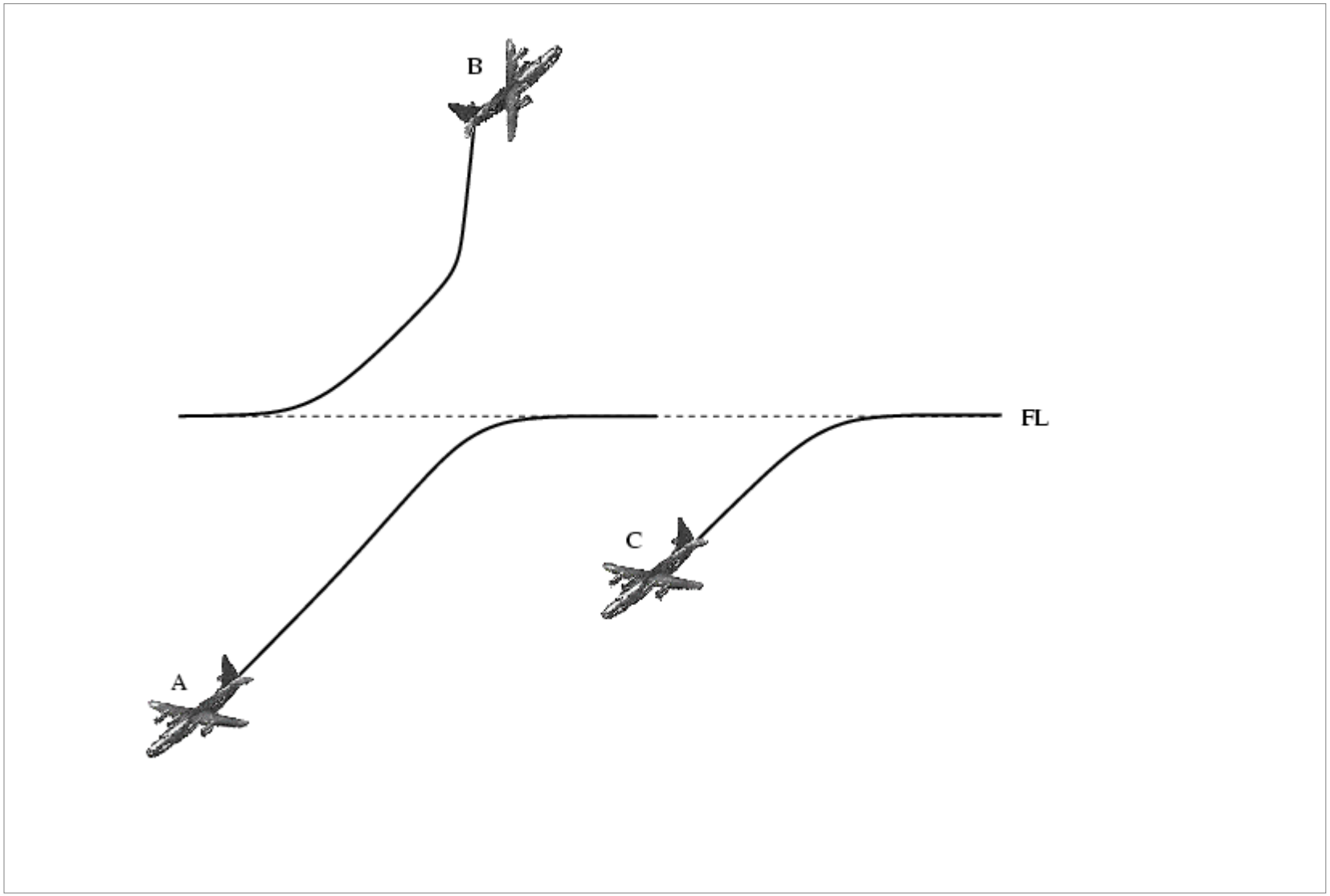
Situation 1: Alternative Resolution



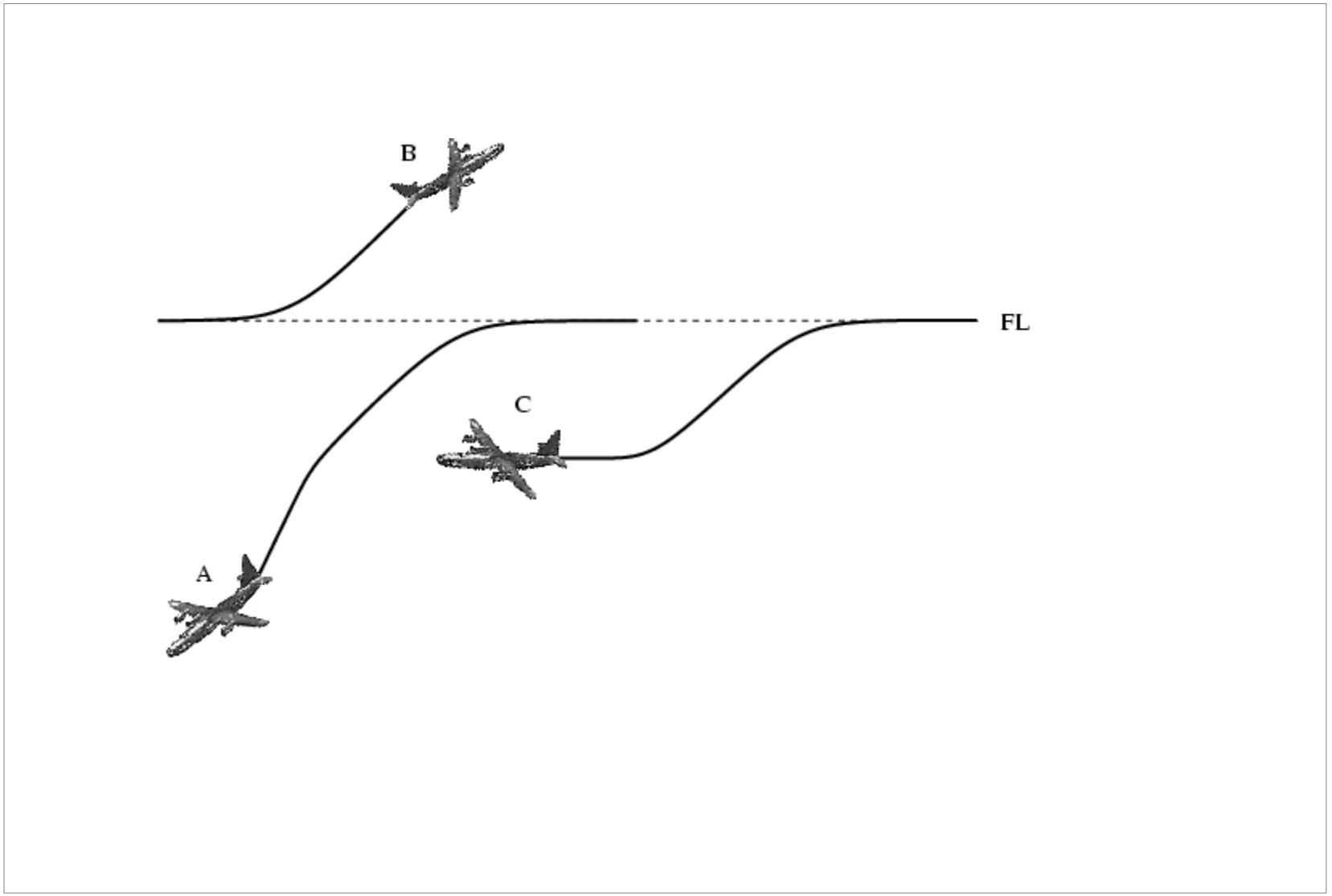
Three−Aircraft Conflict: Situation 2



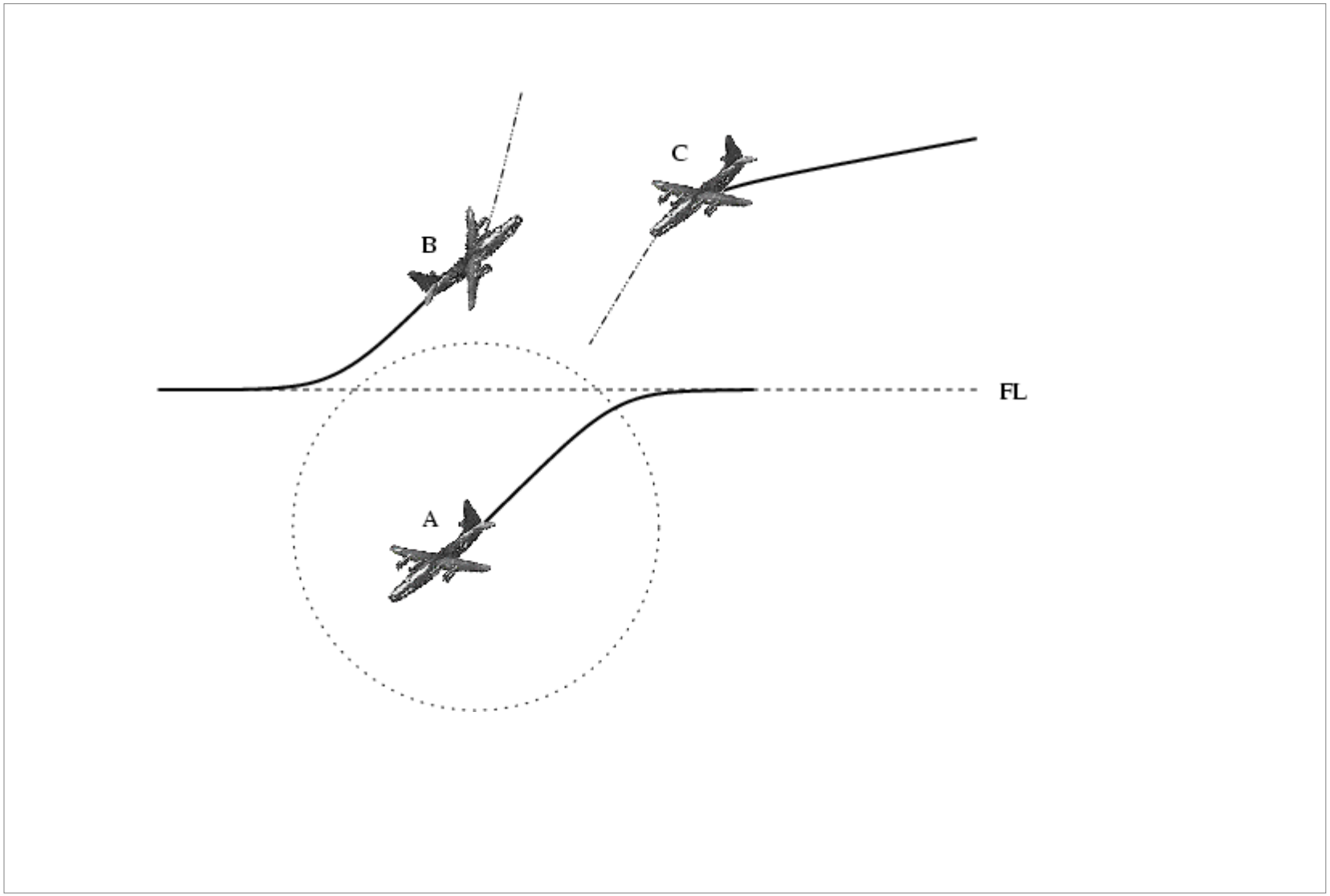
Situation 2: Resolution



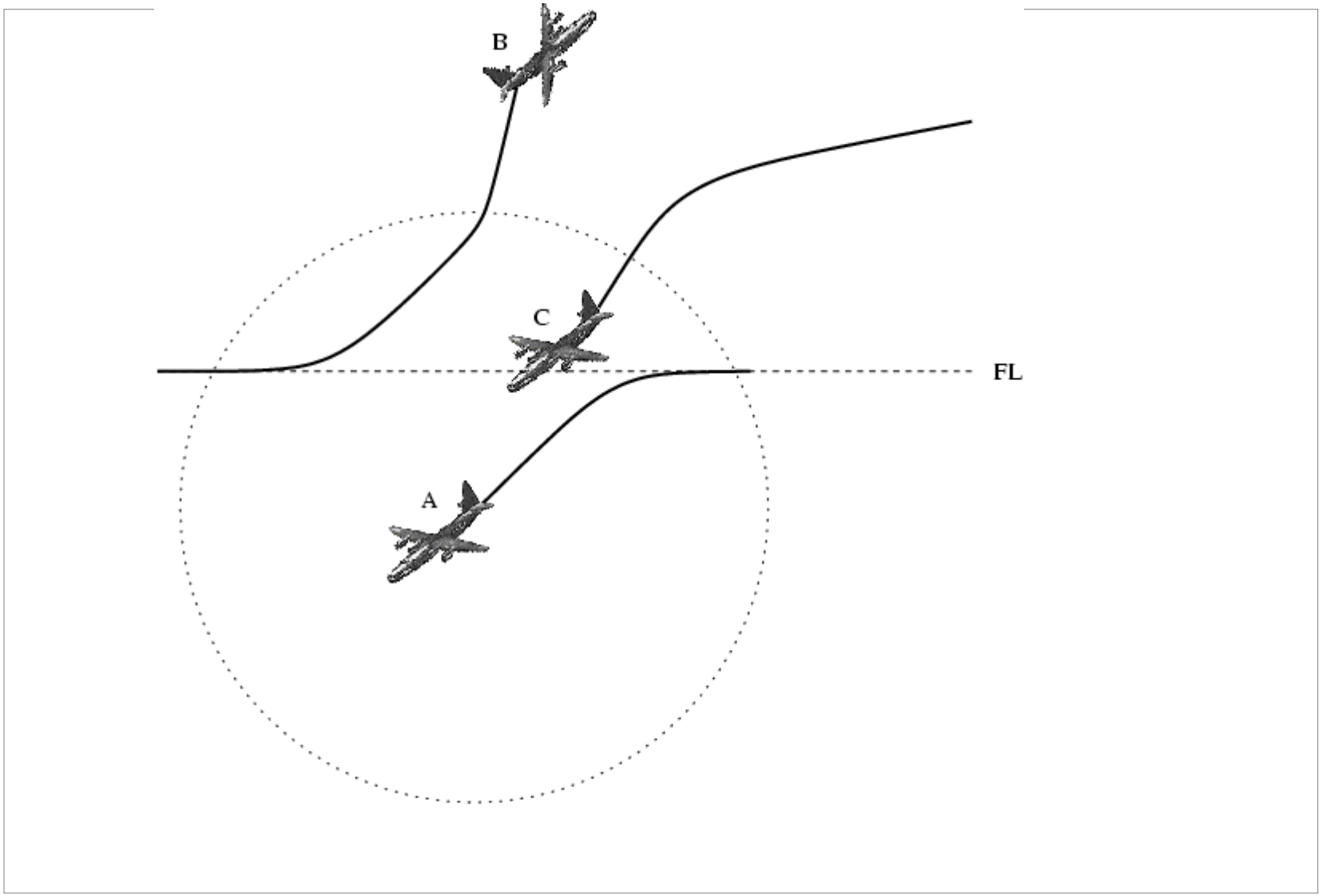
Situation 2: Further Resolution



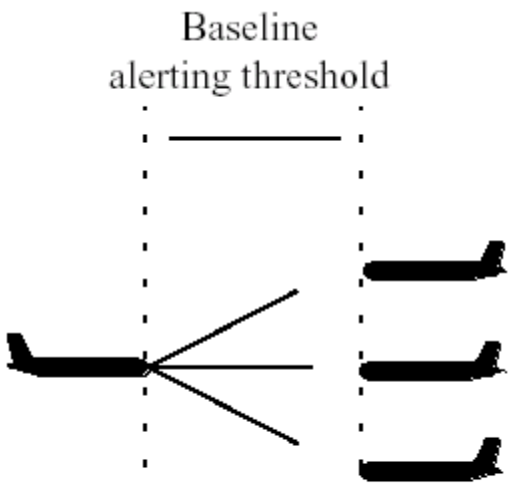
Three−Aircraft Conflict: Situation 3



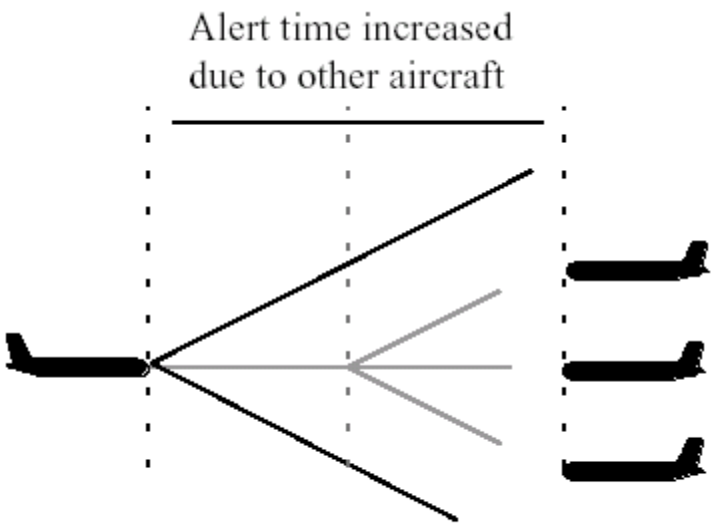
Situation 3: Resolution?



Multiple Aircraft in General



Pairwise Solution



Global Solution

Multiple Aircraft in General

- TCAS can resolve all two−aircraft conflicts (Nancy Lynch, John Lygeros, Carolas Livadas)
- A global solution requires alerts in advance of alerts from pairwise−resolution algorithms (Jim Kuchar)
- Is there a three−aircraft situation in which TCAS **cannot** be shown to resolve conflict?

  I believe so, as shown.

The South German Midair

- Eurocontrol literature advises pilots always to follow an RA
- ICAO position is that one should not manoeuvre in the opposite sense to an RA
- UK CAA position is also "should" rather than "shall". They say: ".. to allow for Commander's discretion to cater for those very limited cases where use of such discretion avoids an incident where the following of ACAS advice may make matters worse"

The South German Midair

- Note that the UK CAA explicitly dissents from the proposition that risk without ACAS majorises risk with ACAS

  (I wonder if they read my commentary?)

The Midair: BTC cognitive state

- TA (traffic approx. position displayed)
- ATC advisory to descend "expedite" for traffic
- RA to climb (traffic displayed at 10 o’clock)
- Second ATC advisory to descend for traffic at "2 o’clock"
- One target you "see"; one target you don’t
- Decision: avoid unseen target by following ATC, try to obtain a visual on displayed target and avoid (night was clear; visual was indeed obtained)

The Midair: Consequences

- "Cognitive state" of BTC crew was constructed from TCAS info + ATC info
- BTC crew cognitive state model substantiates discretionary manoeuvre in contra−sense to Eurocontrol advice
- Pilot−in−Command discretion is enshrined in (UK and US) aviation law
- ACAS system behavior must be analysed with inclusion of ATC advisories (at least)

ACAS System

- ACAS avionics (AV): TCAS II V7 or V6.04a
- Pilot−Flying may not be Pilot−in−Command: resolving RA needs crew (CRW) interaction
- For two−airplane situations there already 4−6 interacting system components: 2 AV, 4 CRW
- AV (2 components of 6) usually the focus of attention

ACAS System

- Example: BFU Statusbericht (Status Report) AX001−1−2/02 August 2002
  - "In beiden Flugzeugen waren die gleichen bordseitigen Zusammenstoßwarngeräte ..... eingebaut. Nach dem derzeitigen Erkenntnisstand wurde keine Fehlfunktion festgestellt"
  - "The same stand−alone collision warning system was built into both aircraft. No failure behavior has been established to date."

ACAS System

- Without CRW, ACAS **does** nothing
- ACAS System is at least: AV + CRW
- CRW behavior regulated by "training"
  - Eurocontrol: Follow the RA! (Bulletin title)
  - ICAO, UK CAA: don’t manoeuvre contrary to RA!

- Previous analysis shows this cannot suffice
  - There is no behavioral algorithm for ACAS
  - Likely there is no universal constraint such as "never manoeuvre contrary to an RA"

ACAS System

- Midair cognitive analysis shows how ATC advisories can help determine (AV + CRW) response to RA
  - (AV + CRW) state includes CRW cognitive state
  - ATC input directly affects CRW cognitive state
  - CRW cognitive state affects aircraft behavior
- Anything which affects system behavior, and over which one has control, can properly be analysed as part of the system

ACAS System

- This reasoning suggests it could be wise to consider the system (AV + CRW + ATC)
  - AV behavior is 2−AC OK, may have 3−AC failure
  - CRW behavior is functionally dependent on CRW cognitive state
  - CRW cognitive state is affected directly by ATC and AV, without a resolution algorithm for contradictory advisories
  - ATC behavior is functionally dependent on ATC cognitive state
  - ATC cognitive state does not include AV state
  - CRW cognitive state includes AV state and ATC advisory
  - Cognitive mistakes (both in state and in communication of state) can be expected

ACAS System State

- Possible: three human components with three different cognitive states, due to one common cognitive mistake in one component

- Zürich ATC:
  +DHL posn, +BTC posn, −RA, −phantom AC
  makes cognitive mistake 10/2 o'clock in advisory

- DHL:
  +DHL posn, +BTC hrz posn, +RA +sense, −phantom AC

- BTC:
  +BTC posn, +DHL hrz posn, +RA +sense, +phantom AC

- A critical system with a single point of failure!

Conclusions

- ACAS AV algorithms have safecrit failures
- ACAS CRW algorithms have safecrit failures
- ACAS−RVSM interactions are safecrit
- RVSM SC does not analyse ACAS−RVSM interactions
- RVSM SC flawed (irreparably)
- One must first recognise the formal problems in order to devise solutions!