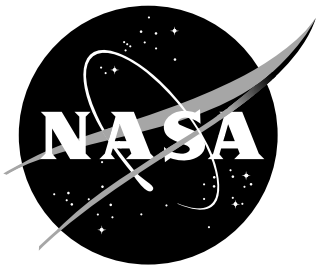
NASA/TM–2010–216862



A Criteria Standard for Conflict Resolution: A Vision for Guaranteeing the Safety of Self-Separation in NextGen

César Muñoz, Ricky Butler, Anthony Narkawicz, Jeffrey Maddalon, and George Hagen
Langley Research Center, Hampton, Virginia

October 2010

NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA scientific and technical information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI Program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI Program provides access to the NASA Aeronautics and Space Database and its public interface, the NASA Technical Report Server, thus providing one of the largest collection of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

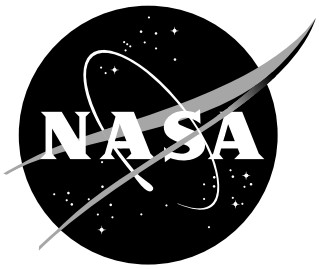
- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers, but having less stringent limitations on manuscript length and extent of graphic presentations.
- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.
- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.
- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.
- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.
- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include creating custom thesauri, building customized databases, and organizing and publishing research results.

For more information about the NASA STI Program, see the following:

- Access the NASA STI program home page at ***http://www.sti.nasa.gov***
- E-mail your question via the Internet to help@sti.nasa.gov
- Fax your question to the NASA STI Help Desk at 443-757-5803
- Phone the NASA STI Help Desk at 443-757-5802
- Write to:
  NASA STI Help Desk
  NASA Center for AeroSpace Information
  7115 Standard Drive
  Hanover, MD 21076–1320

NASA/TM–2010–216862



A Criteria Standard for Conflict Resolution: A Vision for Guaranteeing the Safety of Self-Separation in NextGen

César Muñoz, Ricky Butler, Anthony Narkawicz, Jeffrey Maddalon, and George Hagen
Langley Research Center, Hampton, Virginia

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

October 2010

Available from:

NASA Center for AeroSpace Information
7115 Standard Drive
Hanover, MD 21076-1320
443-757-5802

Abstract

Distributed approaches for conflict resolution rely on analyzing the behavior of each aircraft to ensure that system-wide safety properties are maintained. This paper presents the criteria method, which increases the quality and efficiency of a safety assurance analysis for distributed air traffic concepts. The criteria standard is shown to provide two key safety properties: safe separation when only one aircraft maneuvers and safe separation when both aircraft maneuver at the same time. This approach is complemented with strong guarantees of correct operation through formal verification. To show that an algorithm is correct, i.e., that it always meets its specified safety property, one must only show that the algorithm satisfies the criteria. Once this is done, then the algorithm inherits the safety properties of the criteria. An important consequence of this approach is that there is no requirement that both aircraft execute the same conflict resolution algorithm. Therefore, the criteria approach allows different avionics manufacturers or even different airlines to use different algorithms, each optimized according to their own proprietary concerns.

Contents

1 Introduction **3**

2 Notation **5**

3 Criteria **6**
- 3.1 Horizontal Criterion for Conflict Resolution 7
- 3.2 Horizontal Criterion for Loss of Separation 8
- 3.3 Vertical Criterion for Conflict Resolution 9
  - 3.3.1 Vertical Criterion For Vertical Speed Only 11
  - 3.3.2 The General Vertical Criterion Formula 13
- 3.4 Vertical Criterion for Loss of Separation Recovery 15
- 3.5 3-Dimensional Criteria 16

4 Correctness Theorems **17**
- 4.1 Horizontal Correctness Theorems 17
  - 4.1.1 Conflict Case 17
  - 4.1.2 Loss of Separation Case 18
- 4.2 Vertical Correctness Theorems 20
  - 4.2.1 Conflict Case 20
  - 4.2.2 Loss of Separation Case 20
- 4.3 3-D Correctness Theorems 21

5 Choice of Direction Parameter, ϵ **22**
- 5.1 Horizontal Direction Parameter 23
- 5.2 Vertical Direction 24

6 International Standard for State-Based Coordination **26**

7 Implications for Strategic Algorithms **27**

8 Conclusions **28**

A Summary of Notation **31**

B Summary of Criteria **32**

1 Introduction

Two basic approaches for conflict detection and resolution are being considered for the NextGen Airspace: (1) a centralized concept, where a single authority detects conflicts and makes resolution decisions for several aircraft, and (2) a distributed concept, where the elements of the system make individual decisions about maintaining conflict-free trajectories. There are advantages and disadvantages to each approach, and any future air traffic system will likely have both centralized and decentralized features. If the system is primarily centralized and highly automated, then the safety of the system hinges on assuring the correctness of the software performing the separation function and on many other factors. Alternatively, in a distributed approach the safety of the system cannot just rely on examining the software that is running on the aircraft but must involve analyzing a *distributed* property between the aircraft. For this reason, the safety analysis of a distributed system is probably more complex than a similar analysis for a centralized approach. This paper presents a *criteria* method, which simplifies the analysis of self separation while expanding the possibility of diverse applications.

This criteria method may be used for distributed airspace systems where aircraft execute different resolution algorithms, and it can also be used where each aircraft execute the same algorithm. The second approach was taken in the design of the Traffic Collision Avoidance System (TCAS). A diverse international committee met for many years and came to agreement on the TCAS II algorithm [8]. The first approach is attractive because a large number of resolution algorithms have been proposed in recent years (see [4] for a collection of examples) and it is difficult to imagine that everyone will agree on mandating a single algorithm. The criteria standard allows different avionics manufactures and perhaps different airlines to implement different algorithms, which are optimized for different proprietary goals. All of these algorithms will interact safely, provided that each algorithm is shown to meet the criteria. In this concept the international community agrees on the criteria rather than on a single algorithm. This paper presents proven results that if two algorithms both meet the criteria presented in this paper, then their combined behavior is safe with respect to separation, i.e., the combined effect of their maneuvers resolves the conflict.

This paper introduces criteria that provide strong guarantees of safe separation as long as the aircraft use state-based conflict resolution algorithms that satisfy the common criteria, even when the algorithms are different. Safe separation is guaranteed for all encounter geometries if only one aircraft maneuvers or if both aircraft maneuver to avoid the conflict. When both aircraft maneuver to avoid a conflict, we must ensure that the combination of the maneuvers is safe. One way to achieve this coordinated behavior is for the aircraft to

explicitly communicate their intentions: "I will climb, so you should descend." However, we focus on the concept of *implicit coordination*, which means that when two aircraft maneuver, the combined effect resolves the conflict without any additional communication between them. Only ADS-B surveillance data that is periodically broadcast by all appropriately equipped aircraft is used in implicit coordination. The concept presented here will guarantee implicit coordination for arbitrary combinations of tactical guidance maneuvers (e.g., track only, ground speed only, vertical speed only). For example, one aircraft may select a ground-speed solution and the other aircraft a track-only solution, and the combined effect will still maintain separation. There are several other advantages that accrue from the implicit coordination approach, including: (1) less demand on the radio frequency spectrum, (2) the concept is procedurally simpler and hence less error prone, and (3) less workload on the pilot and controllers.

This paper presents a framework for facilitating the verification of many different algorithms in a mathematically rigorous way, i.e., via formal methods. The concept is built on the idea of having an intermediate verification layer, called the *criteria layer*. This is illustrated in Figure 1: The top layer (yellow)

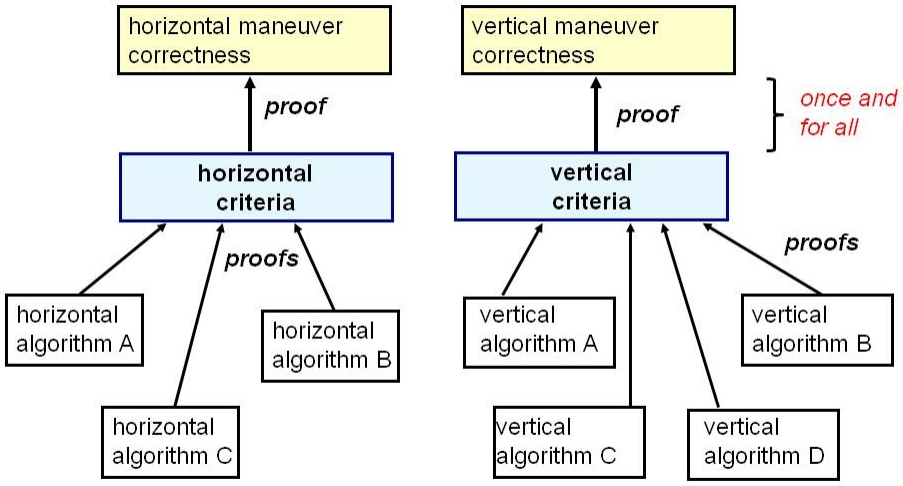


Figure 1. Criteria Concept

defines mathematical correctness for both horizontal maneuvers and vertical maneuvers. The middle layer (light blue) contains the equations that define the *criteria*, and the bottom layer contains the conflict resolution algorithms. The middle layer is the key to achieving our goals. The correctness statements at the top level are state-based, that is, they are specified in terms of the

current position and velocity vectors of the two aircraft. There is no attempt to incorporate intent information in this formulation.

The criteria layer consists of mathematical formulas that are shown to be sufficient to guarantee correctness via formal mathematical proofs. The formulas are analytically defined so that many different algorithms can be checked against the criteria in a straight-forward way. Also, the criteria only use information available to the local aircraft. Each algorithm is then separately shown to satisfy the criteria and thereby inherits the system-wide safety properties. The criteria can also be used as a filter on *any* resolution algorithm that computes multiple solutions. Only solutions that meet the criteria are allowed to be executed and hence this *revised, filtered* algorithm will inherit all of the coordination properties.

This paper proceeds first with a description of notation in Section 2. Section 3 presents individual criteria for different kinds of situations: horizontal conflict resolution, horizontal loss of separation recovery, vertical conflict resolution, and vertical loss of separation recovery. Criteria are also presented that combine the horizontal and vertical criteria in the case of 3-dimensional conflict and loss of separation. Section 4 provides theorems stating that the criteria guarantee independence and coordination. Most resolution maneuvers have two complementary solutions: turn left or right, go up or down, etc. Section 5 describes how an algorithm should choose between these complementary resolutions. In Section 6 there is a discussion about the issues that might arise within an international committee that seeks to adopt the criteria concept. Finally, Section 7 discusses how the criteria standard would work in conjunction with strategic resolution methods that rely on intent information.

The contributions of this paper include: (1) a vision for guaranteeing the safety of the next generation air-traffic management system, based on the criteria approach, (2) the proposal of a specific set of criteria for meeting this vision, and (3) a summary of the mathematical theory used in the criteria.

2 Notation

We consider two aircraft, the *ownship* and the *traffic* aircraft, that are potentially in conflict in a 3-dimensional airspace. The conflict resolution algorithms discussed here only use state-based information, e.g,. initial position and velocity and straight line trajectories, i.e., constant velocity vectors in a Euclidean coordinate system.

We use the following notations:

$\mathbf{s}_o$	3D vector	Initial position of the ownship aircraft
$\mathbf{v}_o$	3D vector	Initial velocity of the ownship aircraft
$\mathbf{s}_i$	3D vector	Initial position of the traffic aircraft
$\mathbf{v}_i$	3D vector	Initial velocity of the traffic aircraft

The components of each vector are scalar values, so they are represented without the bold-face font, for example $\mathbf{s}_o = (s_{ox}, s_{oy}, s_{oz})$. As a simplifying assumption, we regard the position and velocity vectors as accurate and without error. Recent work shows how measurement errors in the state information can be correctly handled by state-based conflict detection and resolution algorithms through the use of appropriate safety buffers [3]. Also, the assumption that the resolutions are executed instantaneously can be mitigated through the use of algorithms that filter infeasible solutions, e.g., algorithms that use models of turn dynamics to determine whether there is sufficient time for a turn to complete.

For notational convenience, all the dot products in this paper are two-dimensional, $\|\mathbf{w}\|$ denotes the norm of the 2-dimensional projection of $\mathbf{w}$, i.e., $\|\mathbf{w}\| = \sqrt{w_x^2 + w_y^2}$, and $\mathbf{w}^2$ denotes $w_x^2 + w_y^2$.

It is mathematically convenient to use a translated coordinate system. The relative position $\mathbf{s}$ of the ownship with respect to the traffic aircraft is defined to be $\mathbf{s} = \mathbf{s}_o - \mathbf{s}_i$, and the relative velocity is denoted by $\mathbf{v} = \mathbf{v}_o - \mathbf{v}_i$. Within this translated coordinate system, the traffic aircraft is at the origin of the coordinate system and does not move. The separation requirements in the airspace systems are specified as a minimum horizontal separation D and a minimum vertical separation H (typically, D is 5 nautical miles and H is 1000 feet). Horizontal and vertical perspectives of this coordinate system are illustrated in Figure 2.

An aircraft trajectory is modeled as a particle with an initial position $\mathbf{s}$, a constant velocity vector $\mathbf{v}$, and a time parameter t. As usually done in state-based conflict detection and resolution, we ignore the effects of wind and only use ground speed in the paper. The location of the aircraft at time t is therefore $\mathbf{s} + t\mathbf{v}$. We will use prime notation to indicate a new velocity vector that is computed by a conflict resolution algorithm, e.g., $\mathbf{v}'$.

3 Criteria

Criteria represent the key safety requirements on the resulting velocity vectors from an airspace separation algorithm. Formally, a *criterion* is a predicate on the set of relative resolution maneuvers. These resolution maneuvers, denoted $\mathbf{v}'$, solve a safety issue related to separation. Two kinds of separation issues are considered in this paper: (1) when the two aircraft are in conflict, i.e., a predicted loss of separation, and (2) when the two aircraft are currently in loss

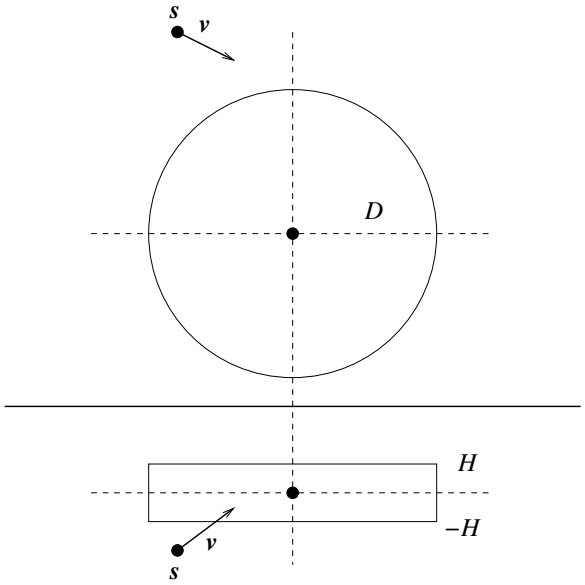


Figure 2. Relative Horizontal and Vertical Perspectives

of separation. If an algorithm ensures that its vectors satisfy a given criterion, then the algorithm correctly solves the separation issue, e.g., in the case of a conflict, the impending conflict is avoided, or in the case of loss of separation, separation is eventually recovered. The criteria are summarized in appendix B.

3.1 Horizontal Criterion for Conflict Resolution

The horizontal criterion for conflict resolution is defined as follows.

Definition 3.1 (`horizontal_criterion`)**.**

$$\texttt{horizontal\_criterion}(\mathbf{s}, \epsilon)(\mathbf{v}') \equiv \mathbf{s} \cdot \mathbf{v}' \geq R\,\epsilon\,\texttt{det}(\mathbf{s}, \mathbf{v}'),$$

where $R = \frac{\sqrt{\mathbf{s}^2 - D^2}}{D}$ and ϵ is a unit value ± 1, which we will call a direction parameter. Any vector $\mathbf{v}'$ that satisfies this formula will resolve the conflict if the traffic aircraft does not maneuver. If both aircraft maneuver, then both aircraft must select resolutions using the same ϵ. This is illustrated in Figure 3. The current ownship velocity vector is shown in blue and the current traffic velocity vector is shown in magenta. If the conflict resolution systems on both aircraft produce resolution vectors anywhere in their green regions, the combined result will be implicitly coordinated. Similarly, if the conflict resolution systems on both aircraft produce resolution vectors anywhere in their blue regions, the combined result will be implicitly coordinated. If only one aircraft maneuvers, then a vector in either the green or blue region will

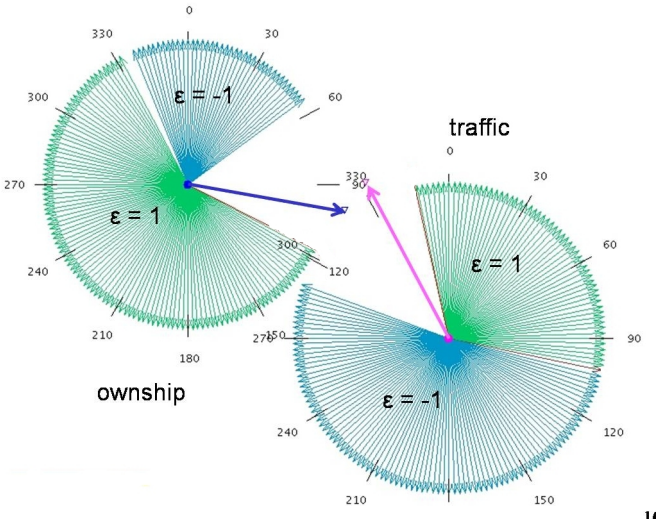


Figure 3. Visualization of Horizontal Criterion for Conflict

suffice. The criterion can also be applied to ground speed solutions. This is illustrated in Figure 4.

A few observations can be made about this criterion. First, it depends on $\mathbf{v}'$, where $\mathbf{v}' = \mathbf{v}'_o - \mathbf{v}_i$, which only uses data that is available locally to an aircraft. In particular, it does not depend upon $\mathbf{v}'_i$, the resolution that will be computed on the traffic aircraft. This is fundamental to achieving implicit coordination, because otherwise an explicit exchange of these computed values would be necessary. Also, although figures 3 and 4 illustrate situations where only one of the ownship's track angle or ground speed changes, the criterion is more general. It applies to velocity vectors $\mathbf{v}'$ where both the ownship's track angle and ground speed change.

3.2 Horizontal Criterion for Loss of Separation

The horizontal criterion for loss of separation is defined as follows.

Definition 3.2 (`horizontal_los_criterion`)**.**

$$\begin{aligned}&\texttt{horizontal\_los\_criterion}(\mathbf{s}, \mathbf{v}, T_h)(\mathbf{v}') \equiv \\ &\quad \mathbf{s} \cdot \mathbf{v}' \geq \mathbf{s} \cdot \mathbf{v} \wedge \\ &\quad \mathbf{s} \cdot \mathbf{v}' > \texttt{exit\_dot\_min}(\mathbf{s}, T_h),\end{aligned}$$

where

$$\texttt{exit\_dot\_min}(\mathbf{s}, T_h) \equiv \frac{\|\mathbf{s}\|}{T_h}(D - \|\mathbf{s}\|).$$

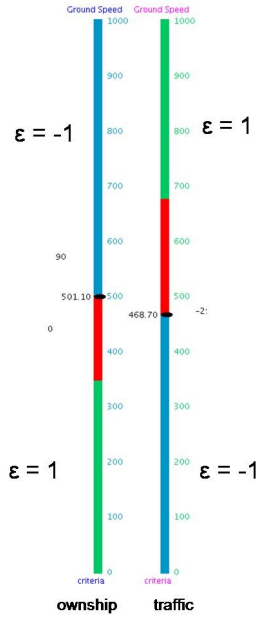


Figure 4. Horizontal Criterion for Ground Speed

If the relative velocity $\mathbf{v}'$ satisfies these two equations, then the criterion is met. Note that the second term implies that the new dot product is positive, which is sufficient to ensure divergence. The second term also ensures that the recovery from the loss of separation is achieved within time T_h. The correctness theorems then ensure that if either aircraft or both aircraft execute a resolution that meets this criterion, then the combined result will be divergence. This is illustrated in Figure 5. The horizontal criterion for loss of separation gives only one region for each aircraft to choose from, namely the green region. In this example the ownship has more options because of its greater ground speed. In Figure 6, we illustrate the impact of the second conjunction of the criterion. The purple region shows the reduced set of vectors that are needed to escape the protection zone within a bounded time.

Once again it should be noted that the criterion only uses data that is available locally on an aircraft. It does not depend upon $\mathbf{v}_i'$ the resolution that will be computed on the traffic aircraft. Thus, an explicit exchange of information is not necessary to achieve safe self-separation.

3.3 Vertical Criterion for Conflict Resolution

The vertical criterion is more complex than the horizontal criterion because it is 3-dimensional. It is certainly possible to create a one-dimensional crite-

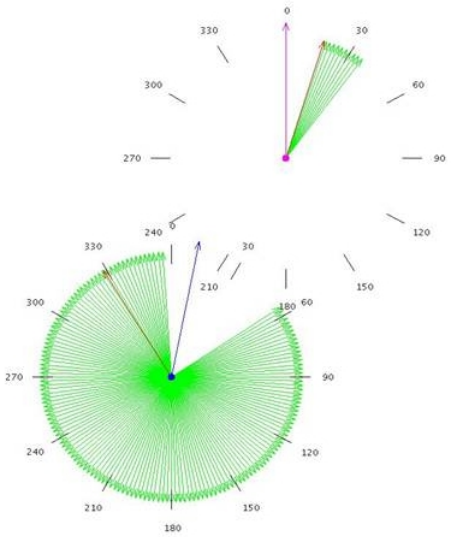


Figure 5. Horizontal Criterion For Loss of Separation Recovery

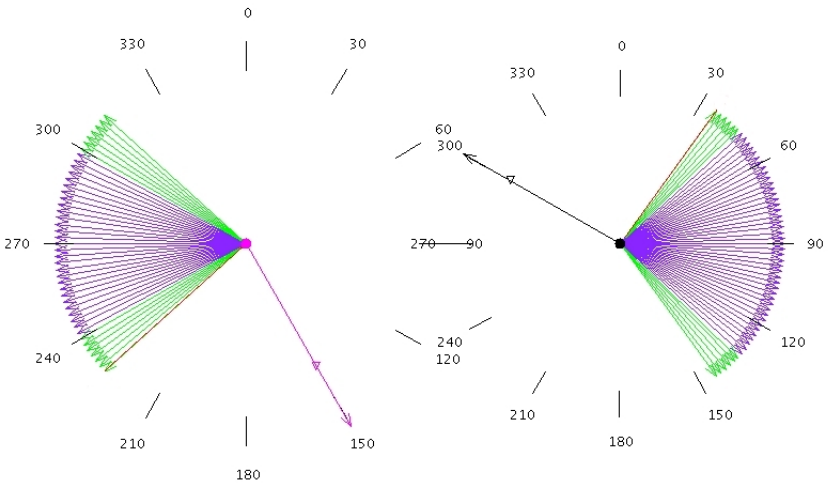


Figure 6. Impact of Second Conjunction of the Criterion

rion that is suitable for vertical-speed-only solutions. However, such a one-dimensional criteria would leave out resolution maneuvers that solve conflicts vertically using ground-speed or track solutions. These kinds of resolutions are possible when the aircraft are already in a climb or descent. In the relative coordinate frame, these solutions fall within a 3-dimensional region of space.

The basic idea is to define a half plane (Figure 7) such that any vector that intersects this plane satisfies the criterion. We will present the formulas

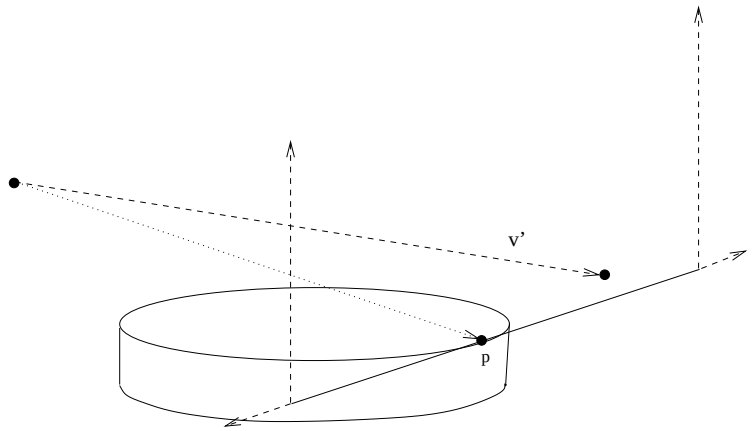


Figure 7. Vertical Criterion

that define this 3-dimensional criteron subsequently, but it is helpful to first examine the criterion for the special cases where only the vertical speed is changed. This special case is one-dimensional.

3.3.1 Vertical Criterion For Vertical Speed Only

There are three basic cases that must be considered:

- Both horizontal and vertical separation exist originally (see Figure 8).
- Only horizontal separation exists originally (see Figure 9).
- Only vertical separation exists originally (see Figure 10).

These regions are determined by the initial position **s** and one of the corners of the protection zone. The horizontal position of a corner is specified using the horizontal entrance/exit times:

- Θ_{-1} = horizontal entrance time.
- Θ_{+1} = horizontal exit time.

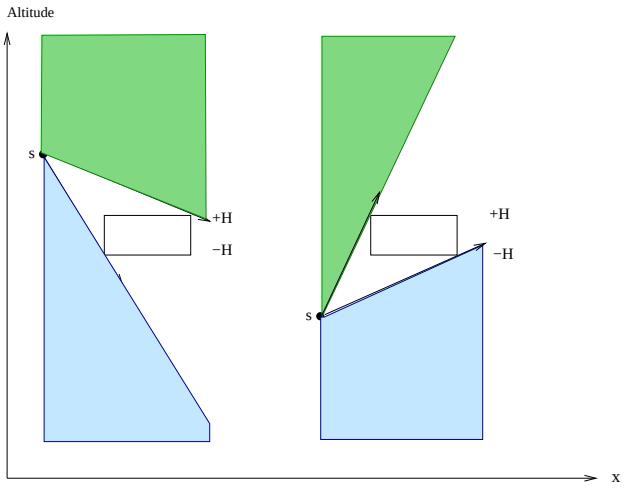


Figure 8. Vertical Criterion Vertical Speed Only Case 1

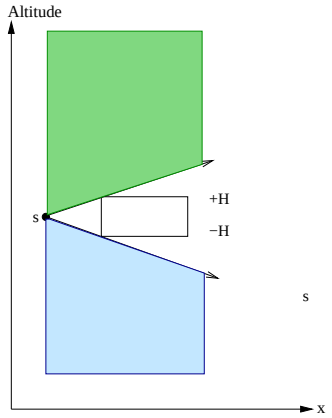


Figure 9. Vertical Criterion Vertical Speed Only Case 2

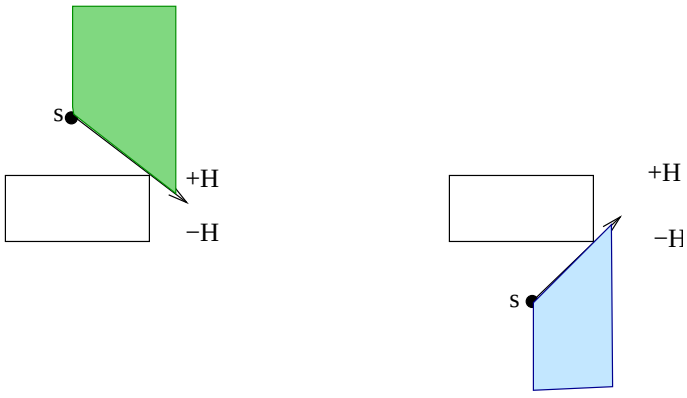


Figure 10. Vertical Criterion Vertical Speed Only Case 3

and the vertical position of a corner is specified with a flag ϵ which indicates top and bottom:

- ϵ = -1 indicates the bottom of protection zone.
- $\epsilon = +1$ indicates the top of protection zone.

Note also that the direction `dir`, whether an entry ($\texttt{dir} = -1$) into the protection zone, or an exit ($\texttt{dir} = +1$) from the protection zone, can be calculated as follows:

$$\texttt{dir} = \texttt{IF } |s_z| \geq H \texttt{ THEN } \epsilon \cdot \texttt{sign}(s_z) \texttt{ ELSE } -1 \texttt{ ENDIF}.$$

Note that the following two formulas

$$|s_z| \geq H \texttt{ AND dir} = \epsilon \cdot \texttt{sign}(s_z)$$

and

$$|s_z| < H \texttt{ AND dir} = -1$$

define the allowed corner points. That is, the border of the criterion region is defined by a line going through these points. The function `sign` returns -1 if its argument is negative and $+1$ otherwise.

3.3.2 The General Vertical Criterion Formula

We will illustrate the concept with the case where there is horizontal separation and $s_z > H$, which is shown in Figure 11. The point $\mathbf{p}$ can be calculated as

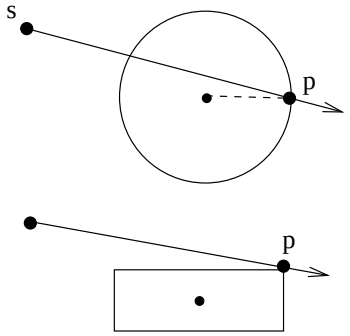


Figure 11. Vertical Criterion Vertical Speed Only Case 3

follows:

$$\mathbf{p} = (\mathbf{s} + \Theta_{+1}\mathbf{v}) \texttt{ WITH } [z \leftarrow \epsilon H],$$

which is $(\mathbf{s}+\Theta_{+1}\mathbf{v})$ with the z component replaced with ϵH. We now construct a line perpendicular to $\mathbf{p}$ (and hence tangent to the circle) as illustrated in

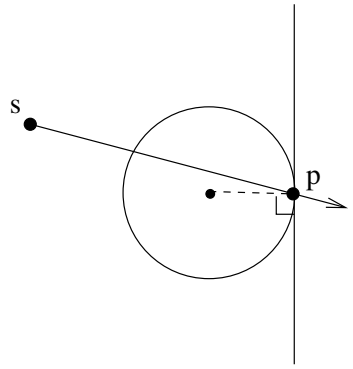


Figure 12. Construction of Tangent Plane

Figure 12. Next, we construct the half-plane that passes through this line and is directly above p_z as illustrated in Figure 7. The vertical criterion states that if a velocity vector $\mathbf{v}'$ from $\mathbf{s}$ intersects this plane, then it is accepted. The plane is completely determined by the point $\mathbf{p}$ and logic specifying which half of the plane is to be used. The point $\mathbf{p}$ defines the vector that is the minimal vertical speed only solution from $\mathbf{s}$. More formally, we can define the vertical criterion as follows.

Definition 3.3 (`vertical_criterion`)**.**

$$
\begin{aligned}
&\texttt{vertical\_criterion?}(\mathbf{s},\mathbf{v},\epsilon)(\mathbf{v}') = \\
&\qquad (\|\mathbf{v}\| = 0 \ \texttt{AND} \ \epsilon\,\mathbf{v}'_z \geq 0 \ \texttt{AND} \ \epsilon\, s_z \geq H \\
&\qquad\ \texttt{OR} \\
&\qquad dir = \texttt{IF} \ |s_z| \geq H \ \texttt{THEN} \ \epsilon \cdot \texttt{sign}(s_z) \ \texttt{ELSE} \ -1 \ \texttt{ENDIF AND} \\
&\qquad \Delta(\mathbf{s},\mathbf{v}) > 0 \ \texttt{AND} \ \Theta_{dir} > 0 \ \texttt{AND} \\
&\qquad \mathbf{p} = (\mathbf{s} + \Theta_{dir}\mathbf{v}) \ \texttt{WITH} \ [z := \epsilon\,\texttt{H}] \ \texttt{AND} \\
&\qquad \texttt{intersects\_half\_plane?}(\mathbf{s},\mathbf{v}',\mathbf{p},\epsilon)).
\end{aligned}
$$

The first term deals with the special case where the *relative* ground speed between the aircraft is zero, i.e., they are flying parallel to each other. The auxiliary function `intersects_half_plane?` is defined as follows:

$$
\begin{aligned}
&\texttt{intersects\_half\_plane?}(\mathbf{s},\mathbf{v},\mathbf{p},\epsilon) = \\
&\qquad \mathbf{v}\cdot\mathbf{p} \neq 0 \ \texttt{AND} \\
&\qquad t = \frac{D^2 - \mathbf{s}\cdot\mathbf{p}}{\mathbf{v}\cdot\mathbf{p}} \ \texttt{AND} \\
&\qquad t \geq 0 \ \texttt{AND} \\
&\qquad \epsilon\,(s_z + t v_z) \geq \epsilon\, p_z,
\end{aligned}
$$

where the dot products are two-dimensional and $\Delta(\mathbf{s}, \mathbf{v}) = D^2\mathbf{v}^2 - (\mathbf{s}^\perp \cdot \mathbf{v})^2$.

This vertical criterion not only includes the vertical-speed only solutions shown in figures 8, 9, and 10, but also vertical resolutions that are achieved by modifying horizontal parameters of the aircraft, i.e., ground speed and track angle. This criterion is illustrated in Figure 13.

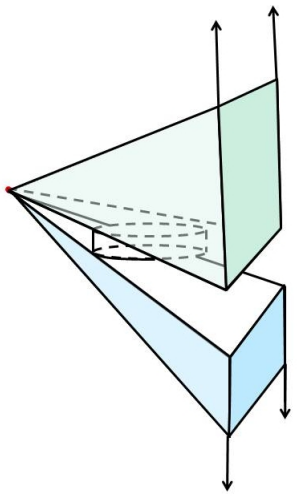


Figure 13. Vertical Criterion: Perspective View

3.4 Vertical Criterion for Loss of Separation Recovery

The vertical loss of separation criterion is only concerned with the vertical component (s_z or v_z) of the position and velocity vectors. A more general 3-dimensional version can be envisioned that would allow horizontal maneuvers that achieve vertical separation when the ownship is currently climbing or descending. Whether such a generalization is desirable operationally is not obvious. This criterion has two components: one to ensure that the aircraft diverge and one to provide a maximum time to recover vertically from the loss of separation. The predicate `vertical_los_criterion?` captures this criterion.

Definition 3.4 (`vertical_los_criterion`)**.**

$$
\begin{aligned}
&\texttt{vertical\_los\_criterion?}(\mathbf{s}, \mathbf{v}, T_v)(\mathbf{v}') = \\
&\quad |s_z| < H \ \texttt{AND} \\
&\quad \texttt{z\_criterion?}(\mathbf{s}, v_z)(v_z') \ \texttt{AND} \\
&\quad T_v \geq \texttt{ttez}(s_z, v_z').
\end{aligned}
$$

The function `ttez` computes the time to exit vertically as follows:

$$\texttt{ttez}(s_z, v_z) = \frac{\epsilon\,\texttt{sign}(v_z)H - s_z}{v_z},$$

for non-zero v_z.

The predicate `z_criterion?` provides one way to guarantees that the two aircraft will diverge.

$$\begin{array}{l}
\texttt{z_criterion?}(\mathbf{s}, v_z)(v_z') = \\
\quad v_z' \neq 0 \ \texttt{AND} \\
\quad \texttt{z_prop?}(s_z, v_z') \ \texttt{AND} \\
\quad (\texttt{z_prop?}(s_z, v_z) \implies \\
\qquad \texttt{IF} \ v_z \neq 0 \ \texttt{THEN} \\
\qquad\quad \texttt{sign}(v_z)\, v_z' \geq 0 \\
\qquad \texttt{ELSE} \\
\qquad\quad \texttt{break_symmetry}(\mathbf{s})\,(v_z') > 0, \\
\qquad \texttt{ENDIF}).
\end{array}$$

where `z_prop?` is defined as

$$\texttt{z\_prop?}(s_z, v_z) = s_z v_z \geq 0,$$

and `sign` returns -1 if its argument is negative and $+1$ otherwise.

The divergence criterion is conceptually simple even though the formal specification is somewhat lengthy. The key idea is contained in `z_prop?`, which sends an aircraft upward if it is higher and downward if it is lower than the other aircraft. The `break_symmetry` function returns a unit value, i.e., ± 1, and is used in the situation where the original vertical speeds are equal (i.e., $v_z = 0$) to overcome the symmetry. It can be any function which satisfies the following two properties:

$$\begin{array}{l}
\mathbf{s} \neq 0 \implies \texttt{break_symmetry}(-\mathbf{s}) = -\texttt{break_symmetry}(\mathbf{s}), \\
s_z \neq 0 \implies \texttt{break_symmetry}(\mathbf{s}) = \texttt{sign}(s_z).
\end{array}$$

3.5 3-Dimensional Criteria

The 3-dimensional criteria that combine the horizontal and vertical criteria for conflict and loss of separation are defined as follows.

Definition 3.5 (`criterion_3D`)**.**

$$\begin{aligned}\texttt{criterion\_3D}(\mathbf{s},\mathbf{v},\epsilon_h,\epsilon_v)(\mathbf{v}') \equiv (&\mathbf{s}^2 \geq D^2 \ \texttt{AND}\\ &\texttt{horizontal\_criterion}(\mathbf{s},\epsilon_h)(\mathbf{v}'))\ \texttt{OR}\\ &(\texttt{vertical\_criterion}(\mathbf{s},\mathbf{v},\epsilon_v)(\mathbf{v}')\ \texttt{AND}\\ &(\mathbf{s}^2 < D^2\ \texttt{OR}\\ &\texttt{horizontal\_criterion}(\mathbf{s},\epsilon_h)(\mathbf{v}'-\mathbf{v}))).\end{aligned}$$

Definition 3.6 (`los_criterion_3D`)**.**

$$\begin{aligned}\texttt{los\_criterion\_3D}(\mathbf{s},\mathbf{v},T)(\mathbf{v}') \equiv &\texttt{horizontal\_los\_criterion}(\mathbf{s},\mathbf{v},T)(\mathbf{v}')\ \texttt{OR}\\ &\texttt{vertical\_los\_criterion}(\mathbf{s},\mathbf{v},T)(\mathbf{v}').\end{aligned}$$

4 Correctness Theorems

The correctness theorems for the conflict case ensure that the resolutions result in conflict free trajectories. The correctness theorems for the loss of separation case establish two key properties:

- Divergence of the two aircraft.
- Timeliness of the recovery, that is separation will be achieved within a specified amount of time.

The theorems in this section are presented without proof. For a presentation of the proofs, see [6].

4.1 Horizontal Correctness Theorems

4.1.1 Conflict Case

The horizontal distance between two aircraft at time t has a simple representation in the relative frame:

$$\begin{aligned}&\sqrt{[(s_{ox}+v_{ox}t)-(s_{ix}+v_{ix}t)]^2+[(s_{oy}+v_{oy}t)-(s_{iy}+v_{iy}t)]^2}\\ &=\sqrt{(s_x+v_xt)^2+(s_y+v_yt)^2}\\ &=\|\mathbf{s}+\mathbf{v}\,t\|.\end{aligned}$$

where $\mathbf{s}$ and $\mathbf{v}$ are 2-dimensional *relative* vectors in the horizontal plane. A *conflict* is a predicted loss of separation. Thus, `horizontal_conflict` can be defined as a loss of separation in the horizontal plane:

Definition 4.1 (`horizontal_conflict`)**.**

$$\texttt{horizontal\_conflict?}(\mathbf{s}, \mathbf{v}) \equiv \exists t : \|\mathbf{s} + \mathbf{v}\, t\| < D.$$

This predicate is true whenever the two aircraft are in conflict. In other words there exists a future time t where a loss of separation will occur.

We can now present the key correctness theorems, when one aircraft maneuvers (independence) and when both aircraft maneuver (coordination).

Theorem 4.1 (`horizontal_criterion_independence`)**.** *If the aircraft are horizontally separated at* $\mathbf{s}$*, then*

$$\texttt{horizontal\_criterion}(\mathbf{s}, \epsilon)(\mathbf{v}) \implies \texttt{NOT horizontal\_conflict?}(\mathbf{s}, \mathbf{v}).$$

The theorem above establishes that the horizontal criterion (Definition 3.1) is sufficient when only one of the aircraft maneuvers. The next theorem states that the horizontal criterion is also adequate when both aircraft maneuver. This is implicit in the fact that the argument to `horizontal_conflict?` is $\mathbf{v}'_o - \mathbf{v}'_i$, which contains both of the new velocity vectors for the ownship and intruder aircraft.

Theorem 4.2 (`horizontal_criterion_coordination`)**.** *If the aircraft are horizontally separated at* $\mathbf{s}$*, then*

$$\begin{aligned}&\texttt{horizontal\_conflict?}(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i)\ \texttt{AND}\\ &\texttt{horizontal\_criterion?}(\mathbf{s}, \epsilon)(\mathbf{v}'_o - \mathbf{v}_i)\ \texttt{AND}\\ &\texttt{horizontal\_criterion?}(-\mathbf{s}, \epsilon)(\mathbf{v}'_i - \mathbf{v}_o)\\ &\implies\\ &\quad \texttt{NOT horizontal\_conflict?}(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}'_i).\end{aligned}$$

The theorem also reveals that it is essential that the unit value $\epsilon = \pm 1$ must be the same for both aircraft in order for there to be coordination. Note that the criterion for the traffic aircraft has arguments that are the negative of the ownship. The position of the traffic aircraft relative to the ownship is $\mathbf{s}_i - \mathbf{s}_o$, which equals $-\mathbf{s}$ and $\mathbf{v}_i - \mathbf{v}_o$, which equals $-\mathbf{v}$.

4.1.2 Loss of Separation Case

For the loss of separation recovery theorems we need to introduce two additional predicates, `horizontal_sep_after?` and `horizontal_divergent?`, which are defined as follows:

Definition 4.2 (`horizontal_sep_after?`)**.**

$$\texttt{horizontal\_sep\_after?}(\mathbf{s}, \mathbf{v}, t) \equiv \\ \forall t' : t' \geq t \implies (\mathbf{s} + t\,\mathbf{v})^2 \geq D^2.$$

This predicate is true if and only if the aircraft are adequately separated for all times greater than t.

Definition 4.3 (`horizontal_divergent?`)**.**

$$\texttt{horizontal\_divergent?}(\mathbf{s}, \mathbf{v}) \equiv \forall t : t > 0 \implies \|\mathbf{s}\| < \|\mathbf{s} + t\mathbf{v}\|.$$

This predicate is true if the distance between the aircraft is strictly increasing for all times greater than t.

The key horizontal loss of separation theorems are:

Theorem 4.3 (`horizontal_los_criterion_independence`)**.**

$$\texttt{horizontal\_los\_criterion?}(\mathbf{s}, \mathbf{v}, T_h)(\mathbf{v}') \\ \implies \\ \texttt{horizontal\_divergent?}(\mathbf{s}, \mathbf{v}') \texttt{ AND} \\ \texttt{horizontal\_sep\_after?}(\mathbf{s}, \mathbf{v}', T_h).$$

Thus, if only one aircraft maneuvers and its algorithm satisfies the criterion, then the two aircraft will be in a divergent state, and within time T_h, they will no longer be in loss of separation. The next theorem covers the case where both aircraft maneuver.

Theorem 4.4 (`horizontal_los_criterion_coordination`)**.**

$$\texttt{horizontal\_los\_criterion?}(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, T_1)(\mathbf{v}'_o - \mathbf{v}_i) \texttt{ AND} \\ \texttt{horizontal\_los\_criterion?}(-\mathbf{s}, \mathbf{v}_i - \mathbf{v}_o, T_2)(\mathbf{v}'_i - \mathbf{v}_o) \\ \implies \\ \texttt{horizontal\_divergent?}(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}'_i) \texttt{ AND} \\ \texttt{horizontal\_sep\_after?}(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}'_i, \texttt{min}(T_1, T_2)).$$

The theorem shows us that if both aircraft's algorithms satisfy the criterion, then the combined result will be implicitly coordinated. This is reflected in the fact that both `horizontal_divergent?` and `horizontal_sep_after?` (in the conclusion) have $\mathbf{v}'_o - \mathbf{v}'_i$ as their parameters (i.e., both of the aircraft's resolutions). Note that the time to exit from the protection zone is the minimum of the two local times T_1 and T_2. Thus, each local aircraft will meet its local timeliness goal.

For examples of formally verified practical algorithms for recovery from loss of separation, the reader is referred to [2].

4.2 Vertical Correctness Theorems

4.2.1 Conflict Case

The vertical correctness theorems in the conflict case are 3-dimensional. They include the case when the velocity vector $\mathbf{v}'$ achieves vertical separation by only modifying the vertical speed, but also the cases when vertical separation is achieved by modifying the horizontal components of $\mathbf{v}'$.

We introduce a predicate `conflict?`, which is true whenever there is a future time where both vertical and horizontal separation is lost:

Definition 4.4 (`conflict?`)**.**

$$\texttt{conflict?}(\mathbf{s},\mathbf{v}) = \exists t : t \geq 0 \ \texttt{AND} \ |s_z + tv_z| < H \ \texttt{AND} \ (\mathbf{s}+t\mathbf{v})^2 < D^2.$$

The key correctness theorems are:

Theorem 4.5 (`vertical_criterion_independence`)**.**

$$\texttt{vertical\_criterion?}(\mathbf{s},\mathbf{v},\epsilon)(\mathbf{v}') \implies \texttt{NOT conflict?}(\mathbf{s},\mathbf{v}').$$

Theorem 4.6 (`vertical_criterion_coordination`)**.**

$$\begin{array}{l}\texttt{conflict?}(\mathbf{s},\mathbf{v}_o-\mathbf{v}_i) \ \texttt{AND} \\ \texttt{vertical\_criterion?}(\mathbf{s},\mathbf{v}_o-\mathbf{v}_i,\epsilon)(\mathbf{v}'_o-\mathbf{v}_i) \ \texttt{AND} \\ \texttt{vertical\_criterion?}(-\mathbf{s},\mathbf{v}_i-\mathbf{v}_o,-\epsilon)(\mathbf{v}'_i-\mathbf{v}_o) \\ \implies \\ \quad \texttt{NOT conflict?}(\mathbf{s},\mathbf{v}'_o-\mathbf{v}'_i).\end{array}$$

The first theorem establishes correctness when only one aircraft maneuvers, and the second theorem establishes correctness when both aircraft maneuver. It is important to note that as long as the ownship uses the unit value $\epsilon = \pm 1$ and the intruder uses the opposite value $-\epsilon$, coordination is guaranteed. We also note that this is different from the horizontal theorems where it is required the unit value ϵ to be the same for the ownship and intruder aircraft.

4.2.2 Loss of Separation Case

As noted in Section 3.4, the vertical loss of separation criterion is one-dimensional. Therefore, we introduce predicates that define divergence and timeliness with respect to the vertical dimension alone. Vertical divergence is defined by `vertical_divergent`:

Definition 4.5 (vertical_divergent)**.**

$$\texttt{vertical\_divergent?}(\mathbf{s}, \mathbf{v}) \equiv \\ \forall t : t > 0 \implies |s_z| < |s_z + t\, v_z|.$$

Definition 4.6 (vertical_sep_after)**.**

$$\texttt{vertical\_sep\_after}(\mathbf{s}, \mathbf{v}, t) \equiv \\ |s_z + t\, v_z| > H.$$

These predicates appear in the correctness theorem to ensure that there is divergence in the vertical dimension and that recovery will be achieved within a maximum time, say T_v. The vertical loss of separation theorems provide results for both the independent and the coordinated cases:

Theorem 4.7 (vertical_los_criterion_independence)**.**

$$\texttt{vertical\_los\_criterion?}(\mathbf{s}, \mathbf{v}, T_v)(\mathbf{v}') \\ \implies \\ \texttt{vertical\_divergent?}(\mathbf{s}, \mathbf{v}') \texttt{ AND} \\ \texttt{vertical\_sep\_after?}(\mathbf{s}, \mathbf{v}', T_v).$$

Theorem 4.8 (vertical_los_criterion_coordination)**.**

$$\|\mathbf{s}\| \neq 0 \texttt{ AND} \\ \texttt{vertical\_los\_criterion?}(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, T_v)(\mathbf{v}'_o - \mathbf{v}_i) \texttt{ AND} \\ \texttt{vertical\_los\_criterion?}(-\mathbf{s}, \mathbf{v}_i - \mathbf{v}_o, T_v)(\mathbf{v}'_i - \mathbf{v}_o) \\ \implies \\ \texttt{vertical\_divergent?}(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}'_i) \texttt{ AND} \\ \texttt{vertical\_sep\_after?}(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}'_i, T_v).$$

The first predicate rules out the situation where the two aircraft are exactly over each other (i.e., their horizontal distance apart is 0).

4.3 3-D Correctness Theorems

The correctness theorems for the 3-dimensional conflict and loss of separation criteria are stated as follows.

Theorem 4.9 (criterion_3D_independence)**.**

$$\texttt{criterion\_3D?}(\mathbf{s}, \mathbf{v}, \epsilon_h, \epsilon_v)(\mathbf{v}') \implies \\ \texttt{NOT conflict?}(\mathbf{s}, \mathbf{v}').$$

Theorem 4.10 (criterion_3D_coordination)**.**

$$\begin{aligned}
&\texttt{conflict?}(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i) \texttt{ AND} \\
&\texttt{criterion_3D?}(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, \epsilon_h, \epsilon_v)(\mathbf{v}'_o - \mathbf{v}_i) \texttt{ AND} \\
&\texttt{criterion_3D?}(-\mathbf{s}, \mathbf{v}_i - \mathbf{v}_o, \epsilon_h, -\epsilon_v)(\mathbf{v}'_i - \mathbf{v}_o) \\
&\Longrightarrow \\
&\quad \texttt{NOT conflict?}(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}'_i).
\end{aligned}$$

Theorem 4.11 (los_criterion_3D_independence)**.**

$$\begin{aligned}
&\texttt{los_criterion_3D?}(\mathbf{s}, \mathbf{v}, T)(\mathbf{v}') \\
&\Longrightarrow \\
&\quad \texttt{divergent?}(\mathbf{s}, \mathbf{v}') \texttt{ AND} \\
&\quad \texttt{separation_after?}(\mathbf{s}, \mathbf{v}', T),
\end{aligned}$$

where

$$\begin{aligned}
\texttt{divergent?}(\mathbf{s}, \mathbf{v}') \equiv\ & \texttt{horizontal_divergent?}(\mathbf{s}, \mathbf{v}') \texttt{ OR} \\
& \texttt{vertical_divergent?}(\mathbf{s}, \mathbf{v}'), \\
\texttt{separation_after?}(\mathbf{s}, \mathbf{v}', t) \equiv\ & \texttt{horizontal_sep_after?}(\mathbf{s}, \mathbf{v}', t) \texttt{ OR} \\
& \texttt{vertical_sep_after?}(\mathbf{s}, \mathbf{v}', t).
\end{aligned}$$

Theorem 4.12 (los_criterion_3D_coordination)**.**

$$\begin{aligned}
&\texttt{los_criterion_3D?}(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, T_1)(\mathbf{v}'_o - \mathbf{v}_i) \texttt{ AND} \\
&\texttt{los_criterion?}(-\mathbf{s}, \mathbf{v}_i - \mathbf{v}_o, T_2)(\mathbf{v}'_i - \mathbf{v}_o) \\
&\Longrightarrow \\
&\quad \texttt{divergent?}(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}'_i) \texttt{ AND} \\
&\quad \texttt{separation_after?}(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}'_i, \texttt{min}(T_1, T_2)).
\end{aligned}$$

These theorems guarantee that all combinations of horizontal and vertical manuevers are independently correct and that they are implicitly coordinated.

5 Choice of Direction Parameter, ϵ

The criteria presented in Section 3 include a direction parameter ϵ, which is a unit value ± 1. This parameter captures the notion of whether the aircraft should turn to the left or right in the horizontal dimension, or similarly up or down in the vertical dimension. From the standpoint of the criteria, the choice is arbitrary, and either choice is safe. Since either choice is safe, we can choose an epsilon based on other factors, such as minimizing the size of the turn.

The key idea is that the choice of ϵ is just as significant a policy decision as the agreement on the criteria itself.

5.1 Horizontal Direction Parameter

There are many schemes that could be developed for choosing the horizontal unit value ϵ used by both aircraft involved in a pairwise conflict, but it is essential that if `Horizontal_Direction` is the function that chooses the horizontal ϵ, the following property holds:

$$\texttt{Horizontal\_Direction}(\mathbf{s}, \mathbf{v}) = \texttt{Horizontal\_Direction}(-\mathbf{s}, -\mathbf{v}). \quad (1)$$

This is sufficient to ensure that both aircraft will choose the same ϵ for the horizontal case.

One simple schema that satisfies Formula (1) is to mandate that $\epsilon = 1$, i.e., use the green solutions only. Alternatively, we could set $\epsilon = -1$ and only use blue solutions. The use of a simple static method for choosing the horizontal direction parameter, e.g., $\epsilon = -1$, will inevitably leave out useful coordinated solutions. This is illustrated in Figure 14. For this configuration of aircraft,

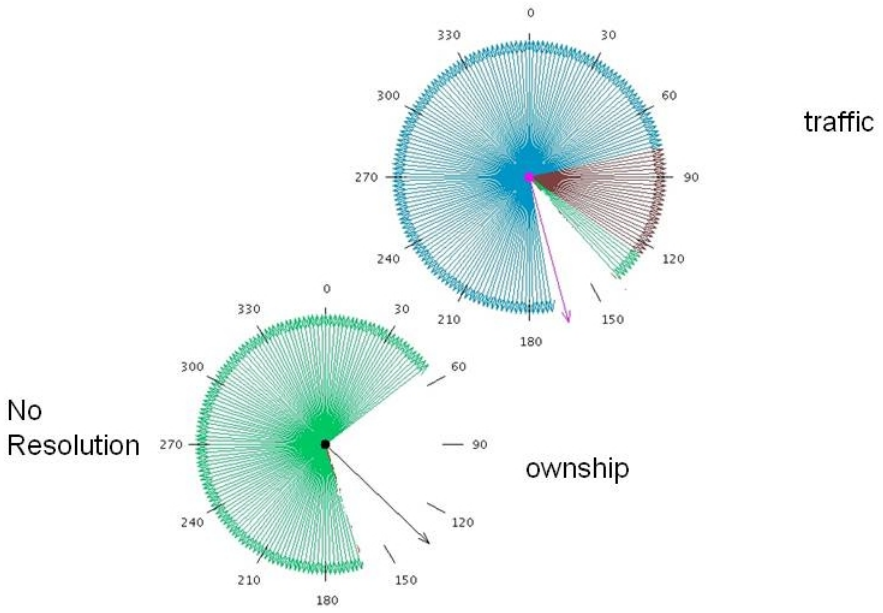


Figure 14. Static ϵ = -1 Direction Problem

there are no blue ($\epsilon = -1$) ownship resolutions. Note that the traffic aircraft has both green and blue resolutions. The brown region is where the green and blue regions overlap. There are other configurations where there are no green solutions.

We recommend the following method:

Definition 5.1 (Preferred Horizontal Direction Parameter)**.**

$$\epsilon = \texttt{sign}(\mathbf{s}^{\perp} \cdot \mathbf{v} \geq 0).$$

This non-static method will sometimes pick a green region and sometimes pick a blue region, as illustrated in Figure 15. The top configuration in Figure 15

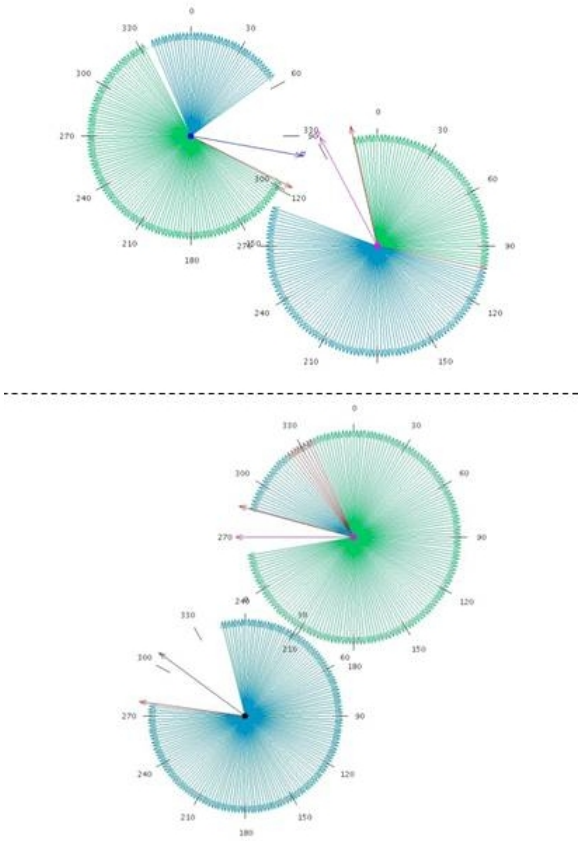


Figure 15. Our Recommended Direction Parameter

results in a green choice while the bottom configuration results in a blue choice. Nevertheless, in all cases the combined result will be implicitly coordinated.

5.2 Vertical Direction

Any function `Vertical_Direction` that chooses a unit value ϵ for the vertical criterion must satisfy

$$\texttt{Vertical\_Direction}(\mathbf{s}, \mathbf{v}) = -\texttt{Vertical\_Direction}(-\mathbf{s}, -\mathbf{v}). \quad (2)$$

This property guarantees that if the ownship chooses a unit value $\epsilon = \pm 1$, the intruder aircraft will choose the opposite value $-\epsilon$.

A simple schema that satisfies Formula (2) is to use $\epsilon = 1$ for the aircraft that is higher, $\epsilon = -1$ for the lower aircraft, and to use a breaking symmetry mechanism if the aircraft are at the same flight level. There are many possibilities for the symmetry breaking function and any can be used as long as the following property holds:

$$\mathbf{s} \neq \mathbf{0} \implies \texttt{break\_symmetry}(\mathbf{s}) = -\texttt{break\_symmetry}(-\mathbf{s}).$$

For example, the following function satisfies the property above:

$$\begin{aligned}\texttt{break\_symmetry}(\mathbf{s}) \equiv \texttt{IF}\ & s_z > 0\ \texttt{OR} \\ & (s_z = 0\ \texttt{AND}\ s_x > 0)\ \texttt{OR} \\ & (s_z = 0\ \texttt{AND}\ s_x = 0\ \texttt{AND}\ s_y > 0) \\ \texttt{THEN}\ & 1 \\ \texttt{ELSE}\ & -1 \\ \texttt{ENDIF}.&\end{aligned}$$

The simple schema is not ideal when the aircraft is currently climbing or descending. Consider the following diagram (Figure 16), where the aircraft is currently descending and is only slightly higher than the other aircraft. In

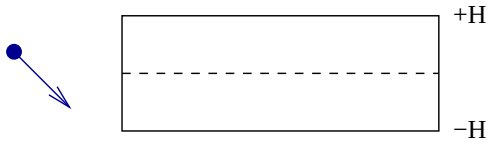


Figure 16. Vertical Criterion: Perspective View

this case it is better to increase the speed of the descent rather than abruptly change directions and climb upward. Thus, we prefer the following method to select the vertical unit value ϵ:

Definition 5.2 (Preferred Vertical Direction Parameter)**.**

$$\begin{aligned}\epsilon = \ & \texttt{IF}\ s_z + \Theta_{-1}\, v_z > 0\ \texttt{THEN}\ 1 \\ & \texttt{ELSEIF}\ s_z + \Theta_{-1}\, v_z < 0\ \texttt{THEN}\ -1 \\ & \texttt{ELSE break\_symmetry}(\mathbf{s}) \\ & \texttt{ENDIF}.\end{aligned}$$

This policy checks the z-component at the time of horizontal entry into the protection zone.

6 International Standard for State-Based Coordination

Under the assumption that distributed self-separation is deemed to have sufficient benefit to the airspace community, an international standard would have to be created and adopted that defines the specifics of the criteria and their application. An important part of the work of this committee will be to develop the requirements that the separation algorithms must meet. These requirements must be evaluated for their safety properties in the manner of a detailed analysis, similar to what was presented in Section 4. The advantage of the criteria standard, which is advocated in this paper, is that it allows efficient investigation of these requirements on algorithms. The efficiency is a result of part of the safety analysis that is done once for all algorithms. If a single algorithm is mandated by the standard then, undoubtedly, multiple algorithm candidates will be evaluated first, so the efficiency of the criteria standard is an important enabling technology. On the other hand, if multiple algorithms are allowed, then the safety requirements are precisely the criteria, along with the associated choice of ϵ (see Section 5).

Understanding the criteria and proofs of correctness requires a certain level of mathematical sophistication. We have attempted to aid the mathematical analysis through the development of a mathematical framework for analyzing criteria and algorithms. We call this framework the Airborne Coordinated Conflict Resolution and Detection (ACCoRD) framework [9]. This framework has been developed with generality in mind. We want to support a wide class of algorithms and criteria. Achieving implicit coordination for both the independent and coordinated cases is non-trivial, and our criteria are by no means unique. Other criteria could be created, but eventually the world community must decide on a set of criteria that will be adopted. Conceivably, the ACCoRD framework may be used for other criteria as well. We believe that our criteria are very general and powerful, but future refinements and improvements are possible. We have at least shown mathematically that such an approach is viable.

All types of analysis rely on certain assumptions, and ACCoRD is no exception. Several idealistic assumptions were made in these proofs: (1) input data contains no errors, (2) the computations were performed with infinite precision, i.e., mathematical real numbers, (3) the resolution maneuvers can be performed instantaneously, and (4) at least one aircraft must implement the prescribed maneuver in a timely manner and the other aircraft must either not change its velocity vector or do so in accordance with the critieria, and (6) only two aircraft are involved in a conflict at the same time. An on-going research effort is underway to enhance ACCoRD by relaxing all of these assumptions. One great advantage of the formal mathematical approach is that the proofs

of correctness can not only be checked by domain experts, but they can also be checked by specialized software called theorem provers. The mathematical proofs in ACCoRD were verified using the PVS theorem prover [7].

7 Implications for Strategic Algorithms

The safety argument for a distributed implementation of self separation is typically built around the idea that there are layers of recovery. Typical layers include (1) strategic conflict resolution, (2) state-based tactical conflict resolution, and finally (3) collision avoidance [1,10]. The strategic conflict resolution system is designed to provide highly efficient solutions but, due to its complexity, it may fail to produce a timely solution. In this case, the system is designed with a backup conflict detection and resolution algorithm that is state-based. If this backup fails to resolve the conflict, then there is a collision avoidance mechanism such as TCAS II to prevent catastrophe. Each system layer contributes to the safety of the system. The strategic layer solves many conflicts and thus the tactical system is invoked infrequently. The tactical layer solves the majority of the remaining conflicts and thus the collision avoidance system is very infrequently invoked. The safety of the system fundamentally depends upon certain correctness properties of these layers, but especially upon the state-based backups. This is precisely where the criteria provide the needed guarantees. The tactical conflict resolution algorithms need only satisfy the conflict criteria to inherit the needed properties. The collision avoidance algorithms need only satisfy the loss of separation criteria.

Strategic algorithms incorporate both the current position and velocity of the aircraft, but also include expected turns, accelerations, decelerations, climbs, and descents. In strategic conflict detection resolution algorithms, coordination is sometimes achieved using different pilot alerting times for the two aircraft. Using this approach, only one aircraft maneuvers at a time. The aircraft with the larger lookahead time is often referred to as the *burdened* aircraft. It is essential that the mechanism for choosing the burdened aircraft be unambiguous and well-defined for all possible configurations of aircraft. We can envision an approach that blends this idea with the criteria approach presented in this paper. While the time to loss of separation is large, only the burdened aircraft maneuvers. However, if the time to loss of separation is small, both aircraft are allowed to maneuver in accordance with the criteria. We would also recommend that the strategic algorithms choose a maneuver (for the burdened aircraft) that is consistent with the criteria. In this way a seamless transition to the state-based algorithms would be achieved. In this blended concept, the criteria serve as a filter on the allowed solutions from the strategic algorithms. In fact, any resolution algorithm can be made consistent with the criteria by using the criteria to filter resolutions.

There is another advantage to using the criteria to filter strategic resolution algorithm solutions: it provides fault tolerance. Suppose that there is some failure in the selection of the burdened aircraft due to data errors or some system failure. If both aircraft erroneously conclude that they are the burdened aircraft, the use of criteria will ensure that the combined result is coordinated.

8 Conclusions

The goal of this work was to develop a mechanism that would allow for the efficient safety analysis of many different separation algorithms. As a consequence of this research, we discovered a way to ensure that aircraft using different conflict resolution algorithms will still have a strong guarantee of aircraft separation. We have shown that a correct algorithm will perform a safe maneuver when both aircraft maneuver at the same time or when only one aircraft executes a maneuver. The mechanism proposed in this paper is the use of an intermediate layer called the criteria layer. For each criterion, the basic idea is to decompose the safety argument into two steps: first, the criterion implies correctness, and second an algorithm satisfies the criterion. The first step establishes that the criterion is sufficient to meet the correctness properties. This verification step has already been accomplished within the ACCoRD framework [9]. We note that if alternate formulas are adopted, the verification would need to be redone. However, some mathematical tools have been developed that could simplify this new verification [6]. The second step shows that a particular algorithm meets the criterion. This must be accomplished for each new algorithm that is developed. We believe that this step is relatively easier than the first step.

For multiple algorithms to be used safely within the distributed concept for self-separation, the international standard must agree on both specific formulas for criteria and a particular method for choosing the direction parameters (ϵ) that appear in the criteria. Some may argue that the proposed criteria are too complex for an international standard to address. We counter that argument with the observation that the criteria here are far simpler than the specification of Traffic Collision Avoidance System (TCAS), whose state machine representation is over 700 pages long [8]. Furthermore, the estimated cost of the TCAS II development over a period of fifteen years was $400 million in 2001 dollars. This estimate includes tests, analyses, and computer simulations [5]. The criteria formulas presented in this paper are complex and a certain level of mathematical sophistication is required to understand them. However, separation systems are complex and safety critical by their nature. We conclude that it will be easier to mandate a set of criteria than attempt to gain international agreement for the development of a single algorithm.

We have sought to make the criteria as general as possible, though we

expect that improvements will continue to be made. An air transportation system built around a criteria standard will be far more general and flexible than a concept where a particular algorithm is mandated. Specifically, the criteria standard supports the natural evolution of the air transportation system as better technologies are introduced that enable better algorithms. In an approach where a single algorithm is mandated, changes in technologies require new international committees. However, in the criteria approach, it is only necessary to show that the new algorithm satisfies the criteria. It then inherits the system-wide global guarantees of coordinated resolutions.

Additionally, the criteria may be used in other contexts. For instance, the criteria can be displayed on the ground control station so that the controllers have an indication of what the algorithms will do. In fact, this criterion approach is not limited to only distributed separation assurance protocols. It could be applied to ground-based concepts. In this way, as long as the controllers choose resolutions within the criteria, hand-offs between sectors, or even between nations, would be coordinated.

References

1. M.G. Ballin, V. Sharma, R.A. Vivona, E.J. Johnson, and E. Ramiscal. A flight deck decision support tool for autonomous airborne operations. In *Proceedings of the AIAA Guidance, Navigation and Control Conference, Monterey, CA, USA, AIAA*. Citeseer, 2002.

2. Ricky W. Butler and César A. Muñoz. Formally verified practical algorithms for recovery from loss of separation. Technical Report NASA TM-2009-215726, NASA Langley Research Center, NASA LaRC,Hampton VA 23681-2199, USA, Jun 2009.

3. Heber Herencia-Zapana, Jean-Baptiste Jeannin, and César Muñoz. Formal verification of safety buffers for state-based conflict detection and resolution. In *Proceedings of 27th International Congress of the Aeronautical Sciences, ICAS 2010*, Nice, France, 2010.

4. James Kuchar and Lee Yang. A review of conflict detection and resolution modeling methods. *IEEE Transactions on Intelligent Transportation Systems*, 1(4):179–189, 2000.

5. MTSI. Airspace modeling for UAS sense and avoid, 2007. http://www.uvs-info.com/Yearbook2007/147_MTSI_Sense-&-Avoid.pdf (accessed Oct. 2000).

6. Anthony Narkawicz and César A. Muñoz. State-based implicit coordination and applications. NASA TP, NASA Langley Research Center, October 2010. Submitted.

7. Sam Owre, John Rushby, and Natarajan Shankar. PVS: A prototype verification system. In Deepak Kapur, editor, *11th International Conference on Automated Deduction (CADE)*, volume 607 of *Lecture Notes in Artificial Intelligence*, pages 748–752, Saratoga, NY, June 1992. Springer Verlag.

8. RTCA. Minimum operational performance standards for traffic alert and collision avoidance system II (TCAS II), 1997. DO-185A.

9. NASA Langley Formal Methods Team. Airborne coordinated conflict resolution and detection (ACCoRD), 2010. http://shemesh.larc.nasa.gov/people/cam/ACCoRD/.

10. David J. Wing, Robert A. Vivona, and David A. Roscoe. Airborne tactical intent-based conflict resolution capability. In *9th AIAA Aviation Technology, Integration, and Operations Conference (ATIO)*, Hilton Head, South Carolina, USA, September 2009.

Appendix A

Summary of Notation

`break_symmetry`	function used to break vertical symmetry
`conflict?`$(\mathbf{s}, \mathbf{v})$	true if aircraft are in conflict horizontally and vertically
`criterion_3D`	the 3-dimensional criterion for conflict resolution
D	diameter of protection zone around an aircraft
$\Delta(\mathbf{s}, \mathbf{v})$	discriminant of quadratic equation from $\|\mathbf{s}+t\mathbf{v}\|^2 = D^2$
`det`$(\mathbf{s}, \mathbf{v})$	$s_x v_y - s_y v_x$
`horizontal_divergent?`$(\mathbf{s}, \mathbf{v})$	true if horizontal distance between two aircraft is increasing
ϵ	± 1, the direction parameter
`exit_dot_min`$(\mathbf{s}, t)$	$\frac{\|\mathbf{s}\|}{t}(D - \|\mathbf{s}\|)$
H	height of protection zone around an aircraft
`horizontal_criterion`	the criterion for horizontal conflict resolution
`horizontal_los_criterion`	the criterion for horizontal loss of separation recovery
`horizontal_conflict?`$(\mathbf{s}, \mathbf{v})$	true if aircraft are in conflict horizontally
`horizontal_sep_after?`$(\mathbf{s}, \mathbf{v}, t)$	true if aircraft will be horizontally separated after time t
`los_criterion-3D`	the 3-dimensional criterion for loss of separation recovery
Θ_{-1}	horizontal entrance time into protection zone
Θ_{+1}	horizontal exit time from protection zone
`sign`(x)	`IF` $x \geq 0$ `THEN` 1 `ELSE` -1 `ENDIF`
$\mathbf{s}_o$	initial position of the ownship aircraft
$\mathbf{s}_i$	initial position of the traffic aircraft
`vertical_criterion?`	the criterion for vertical conflict resolution
`vertical_los_criterion?`	the criterion for vertical loss of separation recovery
`vertical_sep_after`$(\mathbf{s}, \mathbf{v}'_o, \mathbf{v}'_i, t)$	true iff there is vertical separation after t
`vertical_divergent?`$(\mathbf{s}, \mathbf{v})$	true if vertical distance between two aircraft is increasing
$\|\mathbf{w}\|$	two-dimensional norm of vector $\mathbf{w}$
`z_prop?`$(\mathbf{s}, \mathbf{v})$	$s_z v_z \geq 0$

Appendix B

Summary of Criteria

The following table provides a quick reference summary of the criteria presented in this paper.

	Conflict Resolution	Loss of Separation Recovery
horiz.	$\mathbf{s} \cdot \mathbf{v}' \geq R\,\epsilon\,\mathtt{det}(\mathbf{s}, \mathbf{v}')$	$\mathbf{s} \cdot \mathbf{v}' \geq \mathbf{s} \cdot \mathbf{v} \wedge$ $\mathbf{s} \cdot \mathbf{v}' > \mathtt{exit\_dot\_min(s,T)}$
vert.	$\Delta(\mathbf{s}, \mathbf{v}) > 0 \wedge \Theta_{dir} > 0 \wedge$ $\mathbf{p} = (\mathbf{s} + \Theta_{dir}\mathbf{v})$ WITH $[z \leftarrow \epsilon\,\mathtt{H}] \wedge$ $\mathtt{intersects\_half\_plane?}(\mathbf{s}, \mathbf{v}', \mathbf{p}, \epsilon)$	$\lvert s_z \rvert < H \wedge$ $\mathtt{z\_criterion?}(\mathbf{s}, v_z)(v_z') \wedge$ $T_v \geq \mathtt{ttez}(s_z, v_z')$
3D	$(\mathbf{s}^2 \geq D^2 \wedge$ $\mathtt{horizontal\_criterion}(\mathbf{s}, \epsilon_h)(\mathbf{v}')) \vee$ $(\mathtt{vertical\_criterion}(\mathbf{s}, \mathbf{v}, \epsilon_v)(\mathbf{v}') \wedge$ $(\mathbf{s}^2 < D^2 \vee$ $\mathtt{horizontal\_criterion}(\mathbf{s}, \epsilon_h)(\mathbf{v}' + \mathbf{v})))$	$\mathtt{horizontal\_los\_criterion}(\mathbf{s}, \mathbf{v}, T)(\mathbf{v}') \vee$ $\mathtt{vertical\_los\_criterion}(\mathbf{s}, \mathbf{v}, T)(\mathbf{v}')$

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01-10-2010	Technical Memorandum	

4. TITLE AND SUBTITLE
A Criteria Standard for Conflict Resolution: A Vision for Guaranteeing the Safety of Self-Separation in NextGen

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
César Muñoz, Ricky W. Butler, Anthony Narkawicz, Jeffrey M. Maddalon, and George Hagen

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
411931-02-51-07-01

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
NASA Langley Research Center
Hampton, Virginia 23681-2199

8. PERFORMING ORGANIZATION REPORT NUMBER
L–19932

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSOR/MONITOR'S ACRONYM(S)
NASA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
NASA/TM–2010–216862

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified-Unlimited
Subject Category 03
Availability: NASA CASI (443) 757-5802

13. SUPPLEMENTARY NOTES
An electronic version can be found at http://ntrs.nasa.gov.

14. ABSTRACT

Distributed approaches for conflict resolution rely on analyzing the behavior of each aircraft to ensure that system-wide safety properties are maintained. This paper presents the criteria method, which increases the quality and efficiency of a safety assurance analysis for distributed air traffic concepts. The criteria standard is shown to provide two key safety properties: safe separation when only one aircraft maneuvers and safe separation when both aircraft maneuver at the same time. This approach is complemented with strong guarantees of correct operation through formal verification. To show that an algorithm is correct, i.e., that it always meets its specified safety property, one must only show that the algorithm satisfies the criteria. Once this is done, then the algorithm inherits the safety properties of the criteria. An important consequence of this approach is that there is no requirement that both aircraft execute the same conflict resolution algorithm. Therefore, the criteria approach allows different avionics manufacturers or even different airlines to use different algorithms, each optimized according to their own proprietary concerns.

15. SUBJECT TERMS
air traffic, conflict, detection, resolution, avoidance, formal methods, formal verification, criteria, algorithm, safety

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			STI Help Desk (email: help@sti.nasa.gov)
U	U	U	UU	40	19b. TELEPHONE NUMBER *(Include area code)* (443) 757-5802