Formal Analysis of Extended Well-Clear Boundaries for Unmanned Aircraft

César Muñoz and Anthony Narkawicz*

NASA Langley Research Center, Hampton, Virginia 23681-2199
{cesar.a.munoz,anthony.narkawicz}@nasa.gov

Abstract. This paper concerns the application of formal methods to the definition of a detect and avoid concept for unmanned aircraft systems (UAS). In particular, it illustrates how formal analysis was used to explain and correct unexpected behaviors of the logic that issues alerts when two aircraft are predicted not to be well clear from one another. As a result of this analysis, a recommendation was proposed to, and subsequently adopted by, the US standards organization that defines the minimum operational requirements for the UAS detect and avoid concept.

1 Introduction

One of the major challenges to the integration of Unmanned Aircraft Systems (UAS) into the NAS (National Aerospace System) is the lack of an on-board pilot to comply with US and international legal requirements [5, 8]. In manned aircraft operations, on-board pilots have the responsibility for not "operating an aircraft so close to another aircraft as to create a collision hazard", "to see and avoid other aircraft", and when complying with the particular rules addressing right-of-way, on-board pilots "may not pass over, under, or ahead [of the right-of-way aircraft] unless well clear". To address the safety challenge and establish parallel requirements for UAS, the final report of the Federal Aviation Administration (FAA) Sense and Avoid (SAA) Workshop [3] defined the concept of *sense and avoid* as "the capability of a UAS to remain well clear from and avoid collisions with other airborne traffic." This concept, which is now called *detect and avoid*, has been proposed as a means of compliance with the preceding legal requirements.

In 2013, the RTCA organization established the Special Committee (SC) 228 to provide technical guidance to the FAA for defining minimum operational performance standards for the UAS detect and avoid concept, based on a quantitative definition of the well-clear boundary. The well-clear boundary adopted by RTCA SC-228 is defined by a Boolean formula based on the Resolution Advisory (RA) detection logic of the second generation of the Traffic Alerting and Collision Avoidance System (TCAS II) [2]. To accommodate sensor uncertainty and other conditions, the detect and avoid concept considered by RTCA SC-228

* Authors appear in alphabetical order.

allows for the use of extended well-clear boundaries in the logic that issues alerts when aircraft are predicted to lose well-clear status. This paper presents a formalization of extended well-clear boundaries and the verification of their main properties. In particular, it presents a novel result that explains and corrects a potentially unsafe property of extended well-clear boundaries when their threshold parameters are not properly set. The formal analysis presented in this paper resulted in a recommendation to RTCA SC-228 that has been adopted in the current draft of the Minimum Operational Requirements Standards (MOPS) for UAS.

The mathematical development in this paper has been conducted in the Prototype Verification System (PVS) [7]. For readability, this paper uses mathematical notation instead of concrete PVS syntax. For further information on this formal development, the reader is referred to the directory `WellClear` in the NASA PVS Library.[1]

2 Well-Clear Boundary and Its Extensions

This paper considers two aircraft, called *ownship* and *intruder*, whose states are given by position and velocity vectors in a local East, North, Up (ENU) Cartesian coordinate system. Since it is notationally convenient, horizontal and vertical components of a three-dimensional vector are represented by a two-dimensional vector and a scalar, respectively, and these components are presented in a relative coordinate system where the intruder is at the origin and the ownship moves relative to the intruder.

The set of relative aircraft states that are in well-clear violation, i.e., inside the well-clear boundary, is defined as follows.

$$WCV(\mathbf{s}, s_z, \mathbf{v}, v_z) \equiv HWCV(\mathbf{s}, \mathbf{v}) \wedge VWCV(s_z, v_z), \tag{1}$$

where $\mathbf{s}, \mathbf{v} \in \mathbb{R}^2$ are the respective relative horizontal position and velocity vectors of the aircraft, and $s_z, v_z \in \mathbb{R}$ are the respective relative vertical positions and velocities. Informally, a well-clear violation, characterized by the predicate *WCV*, occurs when the aircraft are in horizontal violation, characterized by the predicate *HWCV*, and in vertical violation, characterized by the predicate *VWCV*. The horizontal and vertical violation predicates are defined as follows.

$$HWCV(\mathbf{s}, \mathbf{v}) \equiv \|\mathbf{s}\| \leq \texttt{DMOD} \vee (HMDF(\mathbf{s}, \mathbf{v}) \wedge 0 \leq \tau_{\text{mod}}(\mathbf{s}, \mathbf{v}) \leq \texttt{TAUMOD}), \tag{2}$$

$$VWCV(s_z, v_z) \equiv |s_z| \leq \texttt{ZTHR} \vee 0 \leq t_{\text{coa}}(s_z, v_z) \leq \texttt{TCOA}, \tag{3}$$

where `TAUMOD` and `DMOD` are horizontal time and distance thresholds, respectively, and `TCOA` and `ZTHR` are vertical time and distance thresholds, respectively. The predicate *HMDF* is called the *horizontal miss-distance filter* and is defined as $HMDF(\mathbf{s}, \mathbf{v}) \equiv d_{\text{cpa}}(\mathbf{s}, \mathbf{v}) \leq \texttt{HMD}$, where `HMD` is the horizontal miss-distance threshold and is usually set to the same value as `DMOD`. The distance function

[1] `https://github.com/nasa/pvslib`.

d_{cpa} computes the projected horizontal distance of the aircraft at their closest point of approach, assuming constant relative horizontal velocity, $\mathbf{v}$, and is formally defined as $d_{\text{cpa}}(\mathbf{s},\mathbf{v}) \equiv \|\mathbf{s} + t_{\text{cpa}}(\mathbf{s},\mathbf{v})\mathbf{v}\|$. The time function t_{cpa} is the time to closest point of approach, which is defined as $t_{\text{cpa}}(\mathbf{s},\mathbf{v}) \equiv -\frac{\mathbf{s}\cdot\mathbf{v}}{\mathbf{v}^2}$, when $\|\mathbf{v}\| \neq 0$, and 0 otherwise. The time function τ_{mod}, called *modified tau*, was introduced in the TCAS II RA logic [4]. In the vector notation used in this paper, modified tau is defined as $\tau_{\text{mod}}(\mathbf{s},\mathbf{v}) \equiv \frac{\texttt{DMOD}^2 - \mathbf{s}^2}{\mathbf{s}\cdot\mathbf{v}}$, when $\mathbf{s}\cdot\mathbf{v} < 0$, and -1 otherwise. The time function t_{coa} computes the time to co-altitude assuming constant relative vertical speed v_z. It is defined as $t_{\text{coa}}(s_z,v_z) \equiv -\frac{s_z}{v_z}$, when $s_z v_z < 0$, and -1 otherwise. The conditions $\mathbf{s}\cdot\mathbf{v} < 0$ and $s_z v_z < 0$ hold when the aircraft are horizontally converging and vertically converging, respectively.

For arbitrary values of DMOD, ZTHR, TAUMOD, and TCOA, with HMD = DMOD, Formula (1) satisfies several operational requirements [6]. The values of these thresholds recommended by the UAS SARP [2] and adopted by the RTCA SC-228 are DMOD = HMD = 4000ft, ZTHR = 450ft, TAUMOD = 35s, and TCOA = 0s. These values were chosen using a collision-risk analysis and acceptability metrics aimed to defining a well-clear boundary that is large enough to avoid safety concerns for controllers and see-and-avoid pilots, but small enough to avoid disruptions to traffic flow [1]. Furthermore, the detect and avoid concept considered by RTCA SC-228 only applies to certain types of UAS and in classes of airspace that are usually below 10,000 ft, that is, Class D, Class E, and perhaps Class G airspace.

The well-clear boundary defined by Formula (1) assumes perfect aircraft state information. To accomodate for uncertainty in the position and velocity information, the RTCA SC-228 requirements for the well-clear alerting logic allows for the use of a larger set of threshold values within some ranges. An *extended well-clear boundary* is characterized by a predicate WCV^* defined by Formula (1), but using parameters $\texttt{DMOD}^* \geq \texttt{DMOD}$, $\texttt{HMD}^* \geq \texttt{HMD}$, $\texttt{ZTHR}^* \geq \texttt{ZTHR}$, $\texttt{TAUMOD}^* \geq \texttt{TAUMOD}$, and $\texttt{TCOA}^* \geq \texttt{TCOA}$. The following property, which is proven in PVS, guarantees that the well-clear boundary, instantiated with standard threshold values, is safely included in any of its extensions.

Theorem 1 (Extension). *WCV is included in WCV^*, i.e., for all relative states $\mathbf{s}, s_z, \mathbf{v}, v_z$, $WCV(\mathbf{s}, s_z, \mathbf{v}, v_z) \implies WCV^*(\mathbf{s}, s_z, \mathbf{v}, v_z)$.*

3 An Unexpected Result When $\texttt{HMD}^* > \texttt{DMOD}^*$

In flight simulations at NASA, an unexpected behavior was observed in the alerting logic. In some converging, non-maneuvering encounters (i.e., aircraft flying converging straight line trajectories), alerts due to predicted violation of an extended well-clear boundary suddenly disappear before the closest-point of approach. This behavior was originally blamed on a possible coding error. To understand the actual explanation of this behavior, it is necessary to review the origins of the τ_{mod} function and the horizontal-miss distance filter in the TCAS II RA detection logic.

The definition of the UAS well-clear boundary in Section 2 closely follows the detection logic of the TCAS II RA algorithm.[2] However, while Formula (1) assumes state information in vector form, which is readily available through modern global positioning systems such as GPS, the family of TCAS devices assumes that aircraft are equipped with active transponders, which provide less precise aircraft state information. Earlier versions of the TCAS alerting logic used a simpler variant of Formula (2): $\|\mathbf{s}\| \leq \texttt{DMOD} \ \vee \ 0 \leq \tau(\mathbf{s},\mathbf{v}) \leq \texttt{TAUMOD}$, where τ is defined as range over closure rate or, in vector form, $-\frac{\mathbf{s}^2}{\mathbf{s}\cdot\mathbf{v}}$ when $\mathbf{s}\cdot\mathbf{v} < 0$ and -1 otherwise.

Two problems may arise with use of the simpler variant of Formula (2). The first problem involves encounters with low closure rates. It holds that τ tends to positive infinity as the aircraft reach the closest point of approach, which is attained when the closure rate is 0, i.e., when $\mathbf{s}\cdot\mathbf{v} = 0$. TCAS II addresses this problem by using a modified version of τ, i.e., τ_{mod}. Both τ_{mod} and τ are approximations of time to closest point of approach, t_{cpa}. Indeed, it has been formally proven that for horizontally converging trajectories whose initial states are outside DMOD, i.e., $\mathbf{s}\cdot\mathbf{v} < 0$, $\|\mathbf{s}\| > \texttt{DMOD}$, and $d_{\text{cpa}}(\mathbf{s},\mathbf{v}) \leq \texttt{DMOD}$, $\tau_{\text{mod}}(\mathbf{s},\mathbf{v}) \leq t_{\text{cpa}}(\mathbf{s},\mathbf{v}) \leq \tau(\mathbf{s},\mathbf{v})$ [6]. In contrast to t_{cpa}, the computations of τ and τ_{mod} can be done without directional information. The second problem involves high closure rates with large miss distances, which creates a high rate of false RA alerts. TCAS II addresses this problem by employing a horizontal miss distance filter [4]. The idea behind the filter is to stop RA issuances when the projected future distance at the closest point of approach will be greater than a given distance HMD. In TCAS II, the value HMD is set to be equal to DMOD. The actual horizontal miss-distance filter in TCAS II employs a sophisticated parabolic range tracker to provide projected range, range rate, and range acceleration. Depending on the quality of the range rate estimate computed by the tracker and other conditions, the TCAS II RA system may disable the use of the horizontal miss distance filter. This is in contrast to the well-clear boundary definition where the horizontal miss-distance filter is never disabled. This may cause situations where aircraft are inside the TCAS II RA boundary, but not inside the well-clear boundary. Hence, in the case of the UAS detect and avoid concept, it is tempting to mitigate this problem by using an alerting logic with an extended well-clear boundary where $\texttt{HMD}^* > \texttt{DMOD}^*$.

One key property that can affect the properties of an extended well-clear boundary is whether τ_{mod}, as a function of time for a straight line relative trajectory, i.e., $\tau_{\text{mod}} : t \to \tau_{\text{mod}}(\mathbf{s}+t\mathbf{v},\mathbf{v})$, is monotonically decreasing before closest point of approach. The following lemma, which is proven in PVS, provides a necessary and sufficient condition for the function τ_{mod} to be monotonically decreasing for straight line trajectories.

Lemma 1. *The function τ_{mod} is monotonically decreasing for straight line trajectories if and only if $\|\mathbf{s}+t\mathbf{v}\| \leq \texttt{DMOD}^*$ for some time t.*

[2] The TCAS II RA logic uses TAUMOD instead of TCOA in the vertical dimension.

Consider an extended well-clear boundary where $\texttt{HMD}^* \leq \texttt{DMOD}^*$. Note that this is actually the case in the current version of the TCAS II RA logic, where $\texttt{HMD}^*$ is equal to $\texttt{DMOD}^*$. If there is an alert, then there must be some t where $\|\mathbf{s}+t\mathbf{v}\| \leq \texttt{HMD}^* \leq \texttt{DMOD}^*$. By Lemma 1, this means that τ_{mod} is *always decreasing*. Its graph is shaped as in Figure 1. In this case, the following theorem, which is proven in PVS, holds.

Theorem 2 (Convergence). *An extended well-clear boundary where* $\texttt{HMD}^* \leq \texttt{DMOD}^*$ *is* convergent, *i.e., for all relative states* $\mathbf{s}, s_z, \mathbf{v}, v_z$, *with* $\mathbf{s}\cdot\mathbf{v} \leq 0$, $s_z v_z \leq 0$, *and either* $v_z = 0$ *or* $s_z \neq 0$, *if* $WCV^*(\mathbf{s}, s_z, \mathbf{v}, v_z)$ *then for all* $0 \leq t \leq t^*$, $WCV^*(\mathbf{s}+t\mathbf{v}, s_z + tv_z, \mathbf{v}, v_z)$, *where* t^* *is* $t_{cpa}(\mathbf{s}, \mathbf{v})$ *if* $v_z = 0$, $t_{coa}(s_z, v_z)$ *if* $\mathbf{v} = 0$, *and, in any other case,* $\min(t_{cpa}(\mathbf{s}, \mathbf{v}), t_{coa}(s_z, v_z))$.

The convergence property guarantees that, in a non-maneuvering encounter, a violation of an extended well-clear boundary, where $\texttt{HMD}^* \leq \texttt{DMOD}^*$, never disappears before closest point of approach.

On the other hand, when $\texttt{HMD}^* > \texttt{DMOD}^*$, there are cases where $\|\mathbf{s} + t\mathbf{v}\| > \texttt{DMOD}^*$ for every possible value of t but where $\|\mathbf{s} + t\mathbf{v}\| < \texttt{HMD}^*$ for some t. Thus, there is some time region where τ_{mod} is increasing. In fact, just before closest point of approach, the numerator of τ_{mod} is negative and its denominator is both negative and *approaching negative infinity*. This case is illustrated in Figure 2. This observation leads to the following theorem, which is also proven in PVS.

Theorem 3. *If* $\texttt{HMD}^* > \texttt{DMOD}^*$, *then there exist relative vectors* $\mathbf{s}, \mathbf{v}$ *such that* $d_{cpa}(\mathbf{s}, \mathbf{v}) < \texttt{HMD}^*$, $\mathbf{s} \cdot \mathbf{v} < 0$, *and* $d_{cpa}(\mathbf{s}, \mathbf{v}) > \texttt{DMOD}^*$. *In these situations, the value of* $\tau_{mod}(t)$ *tends to positive infinity as the aircraft reach the closest point of approach.*

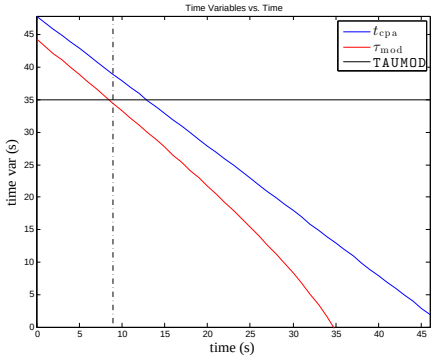

Fig. 1. Case $\texttt{HMD}^* \leq \texttt{DMOD}^*$

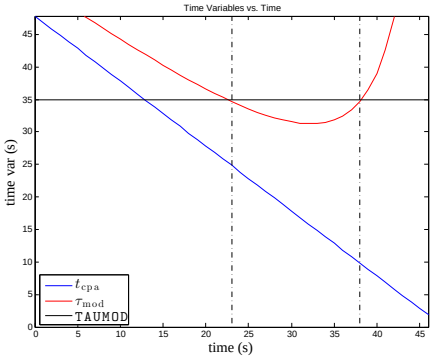

Fig. 2. Case $\texttt{HMD}^* > \texttt{DMOD}^*$

From an operational point of view, a negative consequence of Theorem 3 is that in a non-maneuvering encounter where $\texttt{HMD}^* > \texttt{DMOD}^*$, a violation of an extended well-clear boundary may disappear before the aircraft have reached the closest point of approach. In this case, an alerting logic that protects against such an extended well-clear boundary may unexpectedly stop issuing alerts before the aircraft reach the closest point of approach.

4 Conclusion

This paper reported on the application of formal methods, in particular interactive theorem proving in PVS, to the analysis of extended well-clear boundaries based on the TCAS II alerting logic. In particular, it has been formally proven that an extended well-clear boundary is convergent if $\texttt{HMD}^* \leq \texttt{DMOD}^*$. Furthermore, the analysis explains why, when $\texttt{HMD}^* > \texttt{DMOD}^*$, an alerting logic that protects against such an extended boundary may stop issuing alerts before the aircraft reach the closest point of approach. To the knowledge of the authors, there has been no prior report and explanation of this result. As result of this analysis, the authors recommended to RTCA SC-228 that when an extended well-clear boundary is used by a detect and avoid algorithm, the value of $\texttt{HMD}^*$ is set to $\texttt{DMOD}^*$ (the case $\texttt{HMD}^* < \texttt{DMOD}^*$ is not operationally interesting). This recommendation has been accepted and is part of the current draft of the RTCA SC-228 MOPS for UAS.

References

1. María Consiglio, James Chamberlain, César Muñoz, and Keith Hoffler. Concept of integration for UAS operations in the NAS. In *Proceedings of 28th International Congress of the Aeronautical Sciences, ICAS 2012*, Brisbane, Australia, 2012.
2. Stephen P. Cook, Dallas Brooks, Rodney Cole, Davis Hackenberg, and Vincent Raska. Defining well clear for unmanned aircraft systems. In *Proceedings of the 2015 AIAA Infotech @ Aerospace Conference*, number AIAA-2015-0481, Kissimmee, Florida, January 2015.
3. FAA Sponsored Sense and Avoid Workshop. Sense and avoid (SAA) for Unmanned Aircraft Systems (UAS), October 2009.
4. Jonathan Hammer. Horizontal miss distance filter system for suppressing false resolution alerts, October 1996. U.S. Patent 5,566,074.
5. International Civil Aviation Organization (ICAO). Annex 2 to the Convention on International Civil Aviation, July 2005.
6. César Muñoz, Anthony Narkawicz, James Chamberlain, María Consiglio, and Jason Upchurch. A family of well-clear boundary models for the integration of UAS in the NAS. In *Proceedings of the 14th AIAA Aviation Technology, Integration, and Operations (ATIO) Conference*, number AIAA-2014-2412, Atlanta, Georgia, USA, June 2014.
7. S. Owre, J. Rushby, and N. Shankar. PVS: A Prototype Verification System. In Deepak Kapur, editor, *Proc. 11th Int. Conf. on Automated Deduction*, volume 607 of *Lecture Notes in Artificial Intelligence*, pages 748–752. Springer-Verlag, June 1992.
8. US Code of Federal Regulations. Title 14 Aeronautics and Space; Part 91 General operating and fight rules, 1967.