# Good Fences Make Good Neighbors

## Using Formally Verified Safe Trajectories to Design a Predictive Geofence Algorithm

Yanni Kouskoulas[1], Rosa Wu[1,2], Joshua Brulé[1], Daniel Genin[1], Aurora Schmidt[1(✉)], and T. J. Machado[1,3]

[1] Johns Hopkins University Applied Physics Laboratory, Laurel, USA
aurora.schmidt@jhuapl.edu
[2] Defense Nuclear Facilities Safety Board,Washington, D.C., USA
[3] Department of Mathematics, New Mexico State University, Las Cruces, USA

**Abstract.** For AI-controlled mobile platforms, avoiding collisions with walls and boundaries is an important safety requirement. This is a problem especially for fast-moving aerial vehicles, such as fixed-wing aircraft, that cannot be brought to a stop in an emergency. To enable geographic confinement of such AI-controlled vehicles, we present a formally verified algorithm for predicting geofence violations and selecting a safe maneuver that will keep the vehicle within the designated operations area. The algorithm is based on a higher-order dynamics model that generalizes circular turns using linearly changing centripetal acceleration and allows handling of uncertainty in model parameters. The proposed algorithm was implemented along with extensions to handle non-determinism, and flight-tested on an autonomous aircraft.

## 1 Introduction

There are a host of mobile autonomous and semi-autonomous vehicles being developed today. Examples of these systems include: aerial vehicles used for surveillance and situational awareness, underwater vehicles used for mapping and research of lakes and oceans, surface vehicles used for commercial transport and inspection of bridges, ground vehicles such as autonomous cars and mobile robots. All such systems require a fail-safe confinement mechanism that will prevent them from leaving operations area in case of AI misbehavior.

Geofences are location-defined keep-in/keep-out regions[1]. Geofencing algorithms provide the logic to select actions that limit a system's motion within a geofence. These are especially useful with large and fast moving mobile

[1] For our purposes, we will focus on geofencing for keep-in regions only.

Defense Nuclear Facilities Safety Board—The views expressed herein are solely those of the authors, and no official support or endorsement by the Defense Nuclear Facilities Safety Board or the U.S. Government is intended or should be inferred.

© Springer Nature Switzerland AG 2021
A. Dutle et al. (Eds.): NFM 2021, LNCS 12673, pp. 214–230, 2021.
https://doi.org/10.1007/978-3-030-76384-8_14

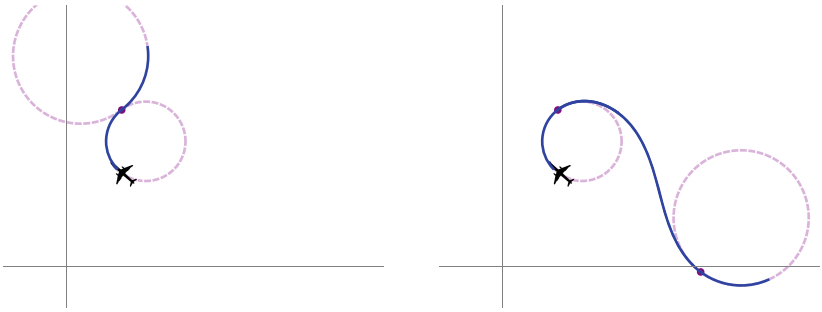
autonomous systems such as jet propelled aircraft, for which physical confinement devices such as barriers and nets are not practical. Most geofencing algorithms in use today are reactive [15,16], i.e. a safety remediation maneuver is triggered when the vehicle crosses a geofence boundary. This means that a geofence cannot be set at the true boundary of a keep-in area since a certain amount of space must be allocated to allow for the remediation maneuver. In order to prevent excursions outside the keep-in area, the interior buffer must be large enough to encompass the safety remediation maneuver, no matter the speed and direction of the motion of the vehicle. In practice, this often means that the resulting geofenced area—allowing unimpeded operation of the vehicle—is significantly smaller than the actual keep-in area, unduly restricting the operational area.

To address this shortcoming of the reactive approach we develop a predictive geofencing algorithm. Rather than waiting for a geofence violation to begin a safety remediation maneuver, our approach is to continuously compute the envelope of possible future positions of the vehicle during a remediation maneuver that is initiated one time step in the future, given its current state. We account for uncertainty in the state estimation, dynamics model and environment, and activate remediation maneuvers only when the future prediction violates the geofence boundary.

Many approaches model vehicle motion using Dubins paths, which are composed of straight lines and circular arcs. However, based on private conversations with experts [13], existing evidence [1], and our own analysis of flight test and simulation data, it is clear that Dubins trajectories deviate from what is actually observed in the fast autonomous aircraft that are the focus of our work. It has also been observed in [2] that differential-drive mobile ground robots have similar deviations from Dubins.

One factor that creates a deviation between modeled and observed trajectories is the change in centripetal acceleration during a turn transition. The dynamics for some vehicles lead to gradual changes in centripetal acceleration during a turn, which doesn't match the step function assumed by the Dubins model. As an improvement, we model a turn transition with a linear ramp in centripetal acceleration. This is a more accurate model – one order higher than Dubins – that more closely matches gradual turn transition dynamics. For vehicles that cannot change their turn rate rapidly, this can make a significant difference in the overall trajectory, as shown in Fig. 1. The kinematics that are produced from such a ramp create a path that follows an Euler spiral [17] (sometimes called Cornu spirals or clothoids).

We develop a mathematically rigorous analysis of the Euler-spiral-augmented Dubins paths that allows us to predict *when* and *which* safety remediation maneuver should be used to keep the vehicle within the geofenced area. The core calculations for analyzing Euler-spiral kinematics are formally verified to guarantee safety, conferring a much higher level of assurance and reliability than is available from other approaches. The analysis is easily converted into a computationally efficient algorithm. By extending the analysis to accommodate uncertainty in state estimation, dynamic model parameters and random environmental factors we make the algorithm robust to errors and noise inevitable in any



(a) Zeroth-order model (b) First-order model

**Fig. 1.** Comparing a path with zeroth- and first-order models for centripetal acceleration changes. The first-order model has an extra curve between the end points of circle arcs created by the linear (vs. discontinuous step) change in centripetal acceleration.

real-world cyber-physical system. Our formal proofs also provide a foundation – a necessary first step – for formally verifying the extensions to the algorithm that are used in the overall approach for even higher levels of reliability.

Finally, we briefly sketch how the algorithm can be used to develop a verified safety fallback controller following ideas developed in [8].

The rest of the paper is structured as follows: in Sect. 3 we develop the analysis of the Euler spiral-augmented Dubins paths.[2] The analysis is subsequently extended to accommodate uncertainty in vehicle state estimation and dynamics model parameters, and random environmental factors (e.g., wind gusts) in Sects. 4. In Sect. 5 we present flight test results of a prototype implementation of the proposed algorithm. We summarize our work and outline directions for future research in Sect. 6.

## 2 Prior Work

There are a variety of challenges associated with enforcing motion boundaries. For example, [15] concentrates on the problem of identifying geofence violations; unlike the present work, it handles combinations of keep-in and keep-out boundaries but provides no predictive dynamics for the vehicle's trajectory and no formal guarantees. Work in [12] combines wavefront-path planning with a vector field describing target orientation to maintain a Dubins path and recover from violations in the presence of fixed obstacles; unlike the present work, the algorithm is grid-based and can handle arbitrary shaped geofences, but is not applicable to vehicles that do not follow Dubins paths and also does not offer

[2] All theorems have been formalized and verified in Coq theorem prover, and are available at https://bitbucket.org/ykouskoulas/egeof-proofs. These proofs rely on the property – admitted as an axiom – that the shortest distance between two points is a straight line.

any formal guarantees. A range of solutions require the creation of inner and outer boundaries to ensure geofence enforcement [4,5]; however, the predictive geofencing algorithm in this work accounts for the aircraft state and future maneuver viability to allow maximum use of space within the geofenced region. This can be a key consideration for ensuring safety on limited sized test-ranges. Predictive geofence violation detection algorithm proposed in [19] uses an innovative approach combining probabilistic aircraft motion model and a viability theory-based approach to predicting violations with high probability. The aircraft motion model, however, is constrained to a linear model, while the approach in the present paper handles nonlinear Euler spiral and Dubins dynamics. In addition, the authors of [19] focus on linear model parameter estimation and cannot guarantee that the obtained model is a strict overapproximation of the aircraft's path, which leads to undetected geofence violations. Our approach seeks to better approximate the path that a fixed wing aircraft follows when performing banked angle turns and seeks to capture the range of future possible positions with non-deterministic envelopes. Finally, to make the approach tractable the authors of [19] had to assume that only one geofence edge would be violated at a time, i.e., violations occur away from corners, while the presented approach handles any number of linear fence constraints simultaneously.

Implementation of motion that respects virtual fixtures in [7] is similar to the geofence problem, but applied to surgical systems. Unlike the present work, the virtual boundaries are planar surfaces oriented in three dimensions and dynamics is for cooperative control with uncertainty; abrupt adversarial acceleration changes are usefully conservative so Euler spirals are not used.

A number of efforts have used Euler spirals to model turning vehicles, but are not formally verified and do not accommodate for envelopes of uncertainty. Euler spirals are used in [2] to create turn transitions; unlike the present work, they are used to smooth existing paths constructed from straight-line segments to allow ground robots to follow them more accurately – obstacle avoidance must be treated separately. In [14], Euler spirals are used to transitions between Dubins turns for path planning; unlike the present work, obstacles are both mobile and cooperative and timing and obstacle avoidance is evaluated by numerical simulation of the path evolution.

Many approaches to horizontal collision avoidance and obstacle avoidance are based on Dubins turns and do not address variations in centripetal acceleration during the turn. For example, [10] searches through a branching set of possibilities to generate 3D Dubins paths for path planning that avoid constant-velocity or stationary obstacles; [18] uses a similar branching search in 2D using a "tentacle" algorithm to find paths that optimize a cost function accounting for turn radii and occupant comfort; and [6] modifies waypoint-based paths by directly calculating additional waypoints based on Dubins-style maneuvers to keep clear of ground obstacles. Unlike the present work, these efforts are not designed to avoid a set of stationary, linear boundaries, and are not formally verified or associated with any guarantees.

The approach we take to developing a controller that uses our proofs to enforce safety in a realistic system is derived from [8], adapted for horizontal motion using a dictionary limited to left/right circling maneuvers; we do not concern ourselves with vertical motion.

Each remediation maneuver in our dictionary ends in a circling trajectory, so the safety computation is similar to [11]. However, this work models gradual changes in centripetal acceleration, so the final circling trajectory is placed differently, and we analyze fixed rather than cooperatively moving obstacles.

## 3 Provably Safe Remediation Maneuvers

In this section we develop the mathematical machinery necessary to determine availability of a safe (with respect to the geofence) turning maneuver with an unlimited time horizon given the current vehicle state. The unlimited time horizon is guaranteed by completing the safe turning maneuver with a provably safe circling pattern that can be maintained until the system is ready to proceed.

The bulk of the work in the current section is devoted to developing properties of Euler spiral turns, since analyzing boundary collisions for the circular path that follows the turn transition is straightforward. The core approach has been formally verified using the Coq proof assistant; each theorem has a corresponding machine-checked proof. We begin by laying down basic assumptions and definitions.

We assume that the vehicle motion is constrained to the horizontal plane, i.e., horizontal motion can be decoupled from vertical motion. This assumption is trivially true for surface vehicles. UAVs (and UUVs) generally maneuver in three dimensions but typically have a control mode that maintains altitude (depth) and allows horizontal control to be effectively decoupled from vertical.

### 3.1 Geofence Representation

We will use geofence to mean a (virtual) boundary made of a non-intersecting curve that divides horizontal plane into a *safe* and *unsafe* regions. We can approximate a geofence boundary with any type of curvature as accurately as necessary with a series of inscribed line segments. We restrict our attention to convex keep-in safe regions, each of which thus approximated can be decomposed into a set of linear boundaries whose union provides a safe approximation.

In practice, geofences are usually specified by providing an ordered list of latitude-longitude pairs corresponding to the vertices of the safe region. We will assume that the safe region is sufficiently small that the curvature of the Earth can be safely ignored. In reality, our computations only require a much weaker assumption, that the safety remediation maneuver path in the flat east-north coordinate system has a negligible error, which is true in all practical situations. The stronger assumption allows us to represent all linear boundaries approximating the safe region as lines in a single Cartesian-coordinate system, which simplifies the presentation.

In our computations, linear geofence segments will be represented as pairs of two dimensional Cartesian points and vectors. A single line passing through point $\mathbf{p} = (p_x, p_y)$ with angular direction $\phi$, measured counterclockwise from the $x$-axis (east) has equation $m_x(y - p_y) = m_y(x - p_x)$, where $m_y = \sin\phi$ and $m_x = \cos\phi$. The corresponding geofence segment will be represented by the pair $(\mathbf{p}, \mathbf{m})$, where $\mathbf{m} = (m_x, m_y)$. In addition, we use the convention that the safe region is always to the left of the line when looking in the direction of $\phi$, or more formally safe region is the set $\{\mathbf{q} | \langle \mathbf{q} - \mathbf{p}, \mathbf{m}^\perp \rangle > 0\}$, where $^\perp$ is the counterclockwise rotation operator defined by $(x, y)^\perp \equiv (-y, x)$.

We also define a safety metric that evaluates the safety of a point $\mathbf{q}$ with respect to a geofence $F = (\mathbf{p}, \mathbf{m})$

$$\text{safe}(\mathbf{q}, F) \equiv \langle (\mathbf{q} - \mathbf{p}), \mathbf{m}^\perp \rangle \tag{1}$$

Simply put, $\text{safe}(\mathbf{q}, F)$ is the signed perpendicular distance from $q$ to the line defining $F$, positive for points left of $F$ and negative for points on the right. Note that safe is defined by exactly the same expression as the safe region. Thus, we have

*Property 1.* $\mathbf{q}$ is in the safe region defined by $F$, or simply safe, if and only if $\text{safe}(\mathbf{q}, F) > 0$.

*Property 2.* The magnitude of $\text{safe}(\mathbf{q})$ is the distance between $\mathbf{q}$ and the closest (via straight-line perpendicular distance) point on the line defined by $F$. Lower valued points are "less safe" than higher valued points.

$$|\text{safe}(\mathbf{q})| = \|\mathbf{m}\| \min_{\langle \mathbf{u}-\mathbf{p}, \mathbf{m}^\perp \rangle = 0} \|\mathbf{q} - \mathbf{u}\| \tag{2}$$

For brevity, $\text{safe}(\mathbf{q})$ will be used when $F$ is clear from context.

A geofence-avoiding safety remediation maneuver is safe if it is entirely contained within the safe geofence region. Since we are restricting our attention to convex geofence regions which are approximated by the intersection of safe half-plane regions, it is enough to check the safety of a maneuver for each linear geofence boundary separately. A maneuver is safe if it is safe for all linear geofence pieces. Thus, it is enough to develop maneuver safety analysis for a single linear geofence. This does not restrict us to solely linear boundaries, as it can ensure safety for curved boundaries and even those with sharp (acute) cusps in the keep-in region.

We next proceed to develop an algorithm for safety analysis of an Euler spiral turn terminating in a circling holding pattern with respect to a single linear geofence. Figure 2(b), shows a turn transition path that is an Euler spiral in which the centripetal acceleration changes linearly based on a finite, constant jerk assumption. To evaluate whether such a maneuver remains on the safe side of a linear boundary, we need to evaluate the safety of the initial turn and the safety of the final circling maneuver. We evaluate safety by finding the least safe (according to the safety metric) point for each of the trajectory segments. Without loss of generality we assume that at the beginning of the maneuver the vehicle is located at the origin and heading east (along the positive x-axis).

### 3.2 Euler Spiral Turns

Creating accurate paths for dynamics with linearly changing centripetal acceleration require curved transitions whose shape is that of an Euler spiral. The Euler spiral is a two-sided, two-dimensional spiral (see Fig. 2(a)) that has applications in areas as diverse as cartography, optics and railroad track construction [9]. It is defined to have a linearly varying curvature, which is the reciprocal of the radius of curvature, and which means that a mass moving with constant speed along an Euler spiral experiences linearly increasing centripetal acceleration, proportional to the distance traveled on the curve. This observation makes it easy to construct Euler spiral turns given initial and final desired centripetal accelerations, e.g., as in when transitioning to a circling pattern. By selecting a subset of the Euler spiral, we can work with a finite-length curve that we can use to model position during a gradual turn. It can represent a smoothly increasing turn, or a transition curve between two different circular arcs. In Cartesian coordinates, the parameterized Euler spiral is given by

$$\xi(k) \equiv \big(\xi_x(k), \xi_y(k)\big) \equiv (\ell C(k/\ell), \ell S(k/\ell)) \tag{3}$$

where $\ell \equiv \sqrt{\pi/\alpha}$, and $\alpha$ is the rate of change of centripetal acceleration in units of $distance/time^3$, and $C(z) \equiv \int_0^z \cos\left(\frac{1}{2}\pi v^2\right) dv$ and $S(z) \equiv \int_0^z \sin\left(\frac{1}{2}\pi v^2\right) dv$ are Fresnel integrals. We use $k$ (standard notation for curvature) to emphasize the relationship between distance and curvature.

These equations give a very convenient arc-length parameterization of the Euler spiral. It follows that the magnitude of parameter $k$ is equal to distance along the curve from the origin, and the sign of $k$ determines the direction of motion – positive to the right and negative to the left. We summarize this in

**Theorem 1 (Euler spiral turn rate).** *After traveling a distance $k$ on the Euler spiral, the radius of curvature at that point is given by $r = 1/(\alpha k)$, corresponding to turn rate $\theta' = \|v\|\alpha k$ (in rad/s) (assuming constant speed $\|v\|$).*

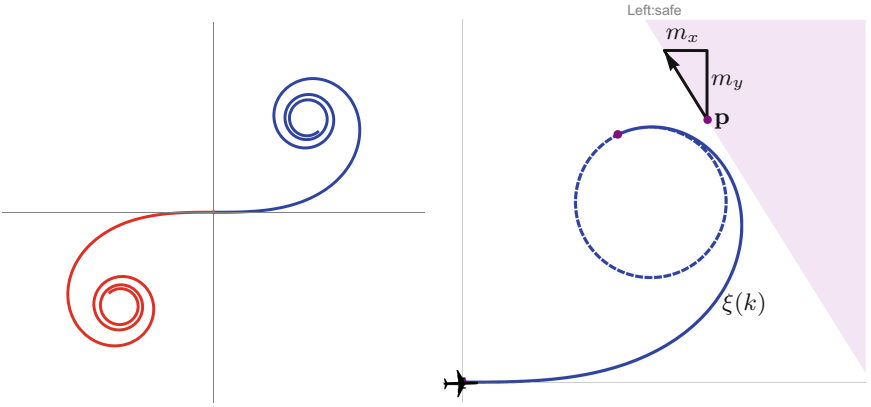
In summary, a transition from straight-line motion to a leftward turn of $\theta'$ rad/s can be represented by a segment of the spiral starting at $k_i = 0$ (the origin) and ending at $k_f = \frac{\theta'}{\|v\|\alpha}$. At the end of the transition, we assume the trajectory follows a circular path shown by the dashed, osculating circle in Fig. 2(b).

Our proofs begin by showing that the Euler spiral is indeed a spiral – something that may or may not have been obvious to Bernoulli when he first started working with these curves – i.e. that further segments of the curve are in some sense contained by the earlier segments of the curve.

**Theorem 2 (Euler spiral is spiral).** *The osculating circle at each point on the right half of the curve $\xi(\cdot)$ contains all the rest of the points in the curve that follow, so that*

$$\forall p, q,\ 0 < p < q \rightarrow \left\| \xi(q) - \left( \xi(p) + \frac{\xi'(p)^{\perp}}{\alpha p} \right) \right\|^2 < \frac{1}{(\alpha p)^2} \tag{4}$$

We approached this by defining an osculating circle, formalizing properties of the Frenet-Serret equations for 2D paths, instantiating those properties for Eq. 3, and then using them to formalize a variant of Kneser's nesting theorem.




(a) Euler spiral (b) Left-turning avoidance maneuver

**Fig. 2.** (a) A full Euler spiral, realized as parametric equation of two Fresnel integrals. We analyze the blue portion of the spiral for a left turn avoidance maneuver. (b) The shaded region represents the area outside the geofence boundary. Initial state starts at the origin traveling straight towards the positive x-axis. The path transitions (solid curve, following $\xi(k)$ from $k \in [k_i, k_f]$) from initial state to circle counterclockwise (dashed curve with radius $r = 1/(\alpha k_f)$). (Color figure online)

### 3.3 Determining Euler Spiral Turn Safety

The Euler spiral has a monotonically changing curvature, with an inflection point at the origin where the turn direction changes from right to left. These properties can be exploited to rigorously evaluate safety of a turn transition by looking at four points along the spiral.

We will define a set of *candidate safety minima* that will include the worst-case dominant point closest to violating the geofence or, if the turn is unsafe, the point deepest into the unsafe region. This set is made up of the points that could be maximally unsafe positions during the maneuver, i.e. the potential minima of the safety metric along the Euler spiral segment. The minimum of a function on a closed interval is either a critical point with positive second derivative or one of the endpoints. The critical points of the safety function can be explicitly computed by setting its derivative to zero

$$\frac{d}{ds}\,\mathrm{safe}\left(\xi(s)\right) = -\cos\left(\frac{\pi}{2}\left(\frac{s}{\ell}\right)^2\right) m_y + \sin\left(\frac{\pi}{2}\left(\frac{s}{\ell}\right)^2\right) m_x = 0 \tag{5}$$

Solving for $s_n$, the $n$th critical point is given by

$$s_n = \begin{cases} \ell\sqrt{\frac{2}{\pi}(\gamma + n\pi)} & \text{for } m_x \neq 0 \wedge n \geq 0 \wedge \gamma \geq 0 \\ \ell\sqrt{\frac{2}{\pi}(\gamma + (n+1)\pi)} & \text{for } m_x \neq 0 \wedge n \geq 0 \wedge \gamma < 0 \\ \ell\sqrt{\frac{2}{\pi}\left(\frac{\pi}{2} + n\pi\right)} & \text{for } m_x = 0 \wedge n \geq 0 \\ -\ell\sqrt{\frac{2}{\pi}(\gamma - (n+1)\pi)} & \text{for } m_x \neq 0 \wedge n < 0 \wedge \gamma \geq 0 \\ -\ell\sqrt{\frac{2}{\pi}(\gamma - n\pi)} & \text{for } m_x \neq 0 \wedge n < 0 \wedge \gamma < 0 \\ -\ell\sqrt{\frac{2}{\pi}\left(\frac{\pi}{2} - (n+1)\pi\right)} & \text{for } m_x = 0 \wedge n < 0 \end{cases} \tag{6}$$

where $\gamma = \tan^{-1}(m_y/m_x)$, which is only sensitive to the sign of the ratio $m_y/m_x$, so $s_n$ enumerates all local extrema. The solutions are indexed so that $n \geq 0$ represent critical points on the right-hand side of the spiral, and $n < 0$ critical points on the left-hand side of the spiral. Note that when the geofence is parallel to the $x$-axis, the inflection point at the origin becomes a critical point of the safety metric and has a double representation as $s_0 = s_{-1}$. Otherwise, each critical point is uniquely determined by its integer index.

The local maxima and minima of the safety function alternate along the spiral as indicated in Fig. 3(a). Key observations that follow from this pattern can be formalized as follows

**Theorem 3 (Critical point safety ordering).** *If $N$ is a positive even integer and $m_y \leq 0$ or $N$ is a positive odd integer and $m_y \geq 0$ then*

$$\text{safe}(s_N) < \text{safe}(s_{N+2})$$

*Moreover, for any two points $s_a < s_b$ in $[s_N, s_{N+1}]$ we have $\text{safe}(s_a) < \text{safe}(s_b)$ and for any $s_a < s_b$ in $[s_{N+1}, s_{N+2}]$, $\text{safe}(s_b) < \text{safe}(s_a)$.*

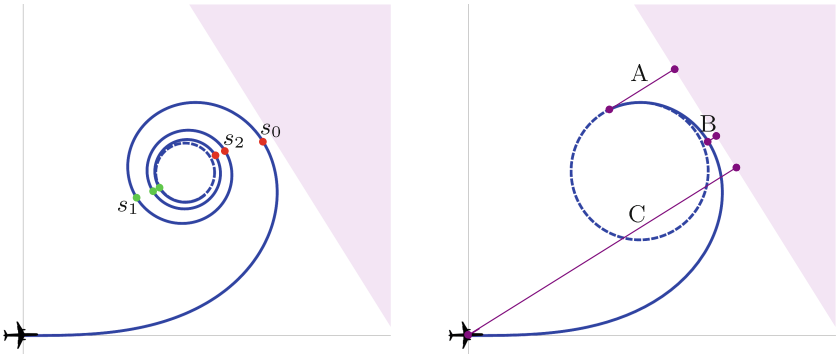
A symmetric result with opposite inequalities holds if the constraints on $m_y$ are reversed (refer to proofs at the provided link for more details). Additional results and detailed reasoning about the $m_y = 0$ case is included in the formal proofs. The corresponding result for $N < 0$ can be deduced from the central symmetry of the Euler spiral about the origin.

Thus, the set of candidate safety minima is the set of positions along the spiral consisting of the endpoints $k_i = 0$ and $k_f = \frac{\theta'}{\|v\|\alpha}$ of the spiral segment (corresponding to the Euler spiral turn), and the set containing at most two critical points with the lowest valued indices contained within the segment $[k_i, k_f]$

$$\mathcal{M} \equiv \{k_i, k_f, \mu_{even}, \mu_{odd}\} \cap \mathbb{R} \tag{7}$$

where

$$\mu_{even} \equiv \inf\{s_{2n} | k_i < s_{2n} < k_f, n \in \mathbb{Z}\}$$
$$\mu_{odd} \equiv \inf\{s_{2n+1} | k_i < s_{2n+1} < k_f, n \in \mathbb{Z}\}$$




(a) Theorem 3 (b) Theorem 4

**Fig. 3.** Theorem visualizations. (a) The critical points of the safety metric, $s_n$, on the Euler spiral alternate between minima and maxima. The points shown in green and red are the local maxima and minima, respectively, of the safety metric. (b) A, B, and C are shortest distances from the critical points of the Euler spiral to the geofence. By Property 2, these distances are proportional to the safety metric; $B < A < C$ so $B$ is the closest approach point by Theorem 4

The intersection with $\mathbb{R}$ is necessary to eliminate potential infinities resulting from the standard convention that $\inf(\varnothing) = \infty$.

Finally, we have the following criterion for determining the safety of an Euler spiral turn:

**Theorem 4 (Euler spiral turn safety).** *An Euler spiral turn, defined by a section of the Euler spiral on parameter interval* $[k_i, k_f]$*, is safe if and only if* $\text{safe}(\mathcal{M}) > 0$*, where* $\text{safe}(\mathcal{M}) = \min_{s \in \mathcal{M}} \text{safe}(s)$*. Moreover, if positive,* $\text{safe}(\mathcal{M})$ *is the distance of the point of closest approach from the geofence, and, if negative, it is the point of the farthest excursion beyond the geofence.*

This follows directly from definitions of safe and $\mathcal{M}$ (Eqs. 1 and 7, respectively), and Theorem 3.

After determining the safety of the Euler spiral turn, analysis of the safety of the final circling pattern is straightforward. Given the center of the terminal circle $\xi(k_f) + (\alpha k_f)^{-1} \xi'(k_f)^{\perp}$, we can determine whether the circumference crosses the geofence.

### 3.4 Arbitrary Initial Conditions

It is straightforward to compute the safety of a turn for a vehicle with arbitrary initial position $\mathbf{q}_0$, $\theta_0$ and $\theta_0'$. We simply need to apply a pair of affine transformations that translate and rotate this initial position and the geofence so that the Euler spiral turn segment of the remediation maneuver lines up with the standard Euler spiral given by $\xi(k)$. To achieve this, we first map the initial position and velocity so that they match up with the origin and the positive $x$-axis respectively. This transformation is defined by $T(\mathbf{q}) \equiv R_{-\theta_0}(\mathbf{q} - \mathbf{q}_0)$, where

$R_\theta$ is the counter-clockwise rotation by $\theta$ given by $R_\theta \equiv \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$. This transforms a geofence defined by $\mathbf{p}$ and $\mathbf{m} = (\cos(\phi), \sin(\phi))$ into $F'$ with $\mathbf{p}' = R_{-\theta_0}(\mathbf{p} - \mathbf{q_0})$, $m'_x = \cos(\phi - \theta_0)$, and $m'_y = \sin(\phi - \theta_0)$.

Next we map this standard initial position of the vehicle and the geofence to the point along the Euler spiral with the matching turn rate. It is easy to compute the correct point because of the linear relationship between distance and curvature for $\xi(k)$. If the initial turn rate is $\theta'_0$ then $k_i = \frac{\theta'_0}{\|v\|\alpha}$. The affine transformation that aligns vehicle in standard position with the corresponding Euler spiral point is $S(\mathbf{q}) = R_\gamma \mathbf{q} + \xi(k_i)$, where $\gamma = \text{atan}_2(\xi'_x(k_i), \xi'_y(k_i))$. So, the composition $S \circ T$, will map the given initial conditions to the corresponding point on the Euler spiral and transform geofence accordingly. The transformed geofence $F'$ has the form: $\mathbf{p}' = R_{\gamma-\theta_0}(\mathbf{p} - \mathbf{q_0}) + \xi(k_i)$, $m'_x = \cos(\phi + \gamma - \theta_0)$, and $m'_y = \sin(\phi + \gamma - \theta_0)$.

The safety of a turn starting with initial conditions $\mathbf{q}_0$, $\theta_0$, $\theta'_0$ with respect to $F$ is equivalent to the safety of the same Euler spiral segment in standard position with respect to $F'$.

Depending on the relationship between the initial and final turn rates, and the direction of the turn, the Euler spiral may need to be traversed in the reverse direction, and one may also need to consider the symmetric Euler spiral $\hat{\xi}(k) = (-\xi_x(k), \xi_y(k))$. It is easy to derive the equivalent of Theorem 3 for $\hat{\xi}(k)$ and the corresponding Theorem 4.

### 3.5 Computational Efficiency

The Euler spiral turn model generalizes the Dubins path model, but remains nearly as computationally efficient for this application. For each safety calculation that evaluates a turning trajectory and a linear boundary, we need to compute, at most, four points – the beginning and end of the Euler spiral segment, and the first two critical points $s_n$, if they fall within the spiral segment of interest. For example, in Fig. 3(b) three critical points will need to checked for safety, the two segment endpoints and the spiral minimum.

Calculating the critical points and evaluating the safety metric at each point involves (a fixed number of) elementary operations, square roots, the `atan2` function, and evaluation of the Fresnel integral, which can be efficiently numerically approximated [3].

In summary, evaluating safety requires linear (in the number of linear segments used to create the geofence boundary) time and no dynamic memory allocations. Safety can be computed for every state update that a controller receives and is practical for real-time applications.

## 4 Extensions to Nondeterministic Trajectories

Until now, we have treated the safety of a specific trajectory. This section describes – without formal proof – extensions to ensure safety for a range of

possible trajectories and a set of boundaries. Each of these extensions may be combined with the others to allow an assessment of safety that includes realistic variations in future possibilities. Whatever procedure we can use to establish safety for a single, linear boundary can be used to establish safety for a set of linear boundaries that we use to safely approximate an arbitrarily curved, convex keep-in area.

*Position Uncertainty.* We can use our analysis to compute safety when knowledge of position in the environment is uncertain. Positional uncertainty may represent sensor noise related to measurement of our absolute position, $(x_0, y_0)$, as well as uncertainty in the exact positioning of the linear boundary $(p_x, p_y)$, or perturbations due to wind during the maneuver. Each of these types of positional uncertainty create an envelope around the aircraft or fence, encompassing a range of possibilities for relative positions for the fence and vehicle.

We add an additional buffer, made by combining these factors into a offset $d$, which quantifies the maximum amount by which our uncertainty can unexpectedly push us closer to the fence during the maneuver. If we choose our reference frame to be fixed on the aircraft these uncertainties shift the fence by $d$ in a direction perpendicular to its orientation, so the linear boundary defined by $\mathbf{p} = (p_x, p_y)$, $m_x = \cos\phi$, and $m_y = \sin\phi$ becomes a linear boundary defined by $\mathbf{p} + d(-m_y, m_x)$. When there is more than one linear boundary that makes up the geofence, each linear boundary must shift the point that defines its position according to its individual $m_x$ and $m_y$ slope components. This shifting of boundaries moves the geofence "inward," giving us a margin of error to safely handle position uncertainty.

*Circling Radius Uncertainty.* The turn radius we use is an upper bound for a safe turn radius. All else equal, smaller turn radii are also safely contained on the safe side of the linear boundary, because the osculating circle at any given point in the Euler spiral contains the rest of the spiral, and also contains any osculating circle that is further along the spiral, as shown in Theorem 2. Any final turn radius we determine to be safe also ensures that any smaller turn radius is also safe.

*Orientation Uncertainty.* We can use our analysis to compute safety when knowledge of our orientation in the environment is uncertain, which may be due to noise related to estimation of our absolute orientation $\theta \in [\theta_l, \theta_h]$ defined by the direction of motion.

We must check the safety of positions within a convex region created by the union of convex hulls associated with the range of spirals possible for the uncertainty in orientation. This union is made from the convex hull for a single orientation $\theta$, rotated around its starting position $(x_0, y_0)$, through the range of possible direction angles $[\theta_l, \theta_h]$. The union is shown for two different turns by the shaded areas in Fig. 4(c). Checking the safety may be done in two steps: first, we check the safety of the convex hulls associated with limiting orientations $\theta_l$ and $\theta_h$; second, check the safety of points within a pie slice shape whose vertex

$(x_0, y_0)$ is connected with line segments to points the furthest points in the limiting hulls connected to each other by a circular arc.

We can find the distance to the furthest point on the curve $\rho_s$ from $(x_0, y_0)$, our present position, by solving for the minimum value of $k$ in $D_s(k) \cdot \frac{d}{dk} \xi(k) = 0$ where $D_s(k) = \xi(k) - \xi(k_i)$ is the vector from the start of the turn to each future position in the trajectory identified by $k$. Recall $k_i$ is the parameter identifying the start point of the spiral segment that models our turn transition. If no such solution exists, then $\rho_s = k_f$. Similarly, we can solve for the furthest point on the turning circle $\rho_c$ from $(x_0, y_0)$ and the distance associated with this point $D_c(\rho_c)$.

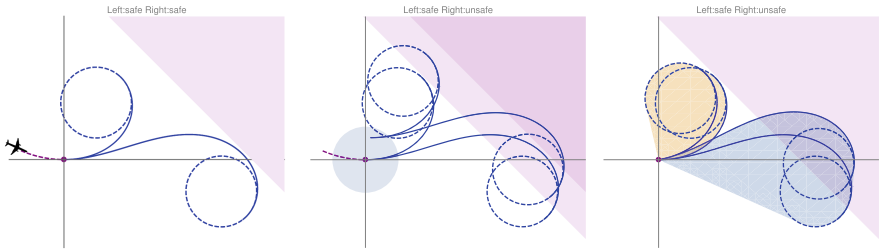
We then find the furthest point for the convex hull at that angle by taking the point associated with the maximum of the two possibilities,

$$f_\theta = \begin{cases} \rho_c \text{ for } \|D_c(\rho_c)\| \geq \|D_s(\rho_s)\| \\ \rho_s \qquad\qquad \text{otherwise} \end{cases} \tag{8}$$

## 5 Application

This project included testing the formally verified predictive geofencing algorithm in a US Air Force flight test. We have implemented our analysis of the Euler spiral turning model as a fallback safety controller which was integrated into an on-board watchdog controller. The predictive geofence violation detection logic was synthesized directly from the technique described in [8]. To ensure that an autonomous vehicle's motion respects a geofence, we created a dictionary of predictive models of its future trajectory, sampling both left and right turns. A remediation maneuver is chosen to be a transition to a circular holding pattern. This ensures that if we remediate, we can continue to safely follow the remediation maneuver for as long as necessary, abandoning it and transitioning to a safe alternative trajectory when one becomes available.

At each time-step, the watchdog evaluates whether we can: allow the present motion (within uncertainty bounds) to continue until the next control time-step and then, at that future time, initiate and follow a remediation maneuver that keeps us within the geofence boundary. While propagating the current state of the plane to a future state at which the remediation might be applied, we incorporate future state uncertainty by allowing a range of possible positions and orientations. If we can ensure at each control time-step that we can initiate remediation at the next control action, then we can allow the autonomy to operate without interference. If we find that the present trajectory cannot be made safe by future remediation, then we immediately initiate remediation in the current control time-step. It is guaranteed safe under our assumptions by the analysis we made during the previous control interval. Figure 4 illustrates the evaluation of the safety of initiating left and right turns in the future for a single trajectory. Our approach can safely handle a range of future possibilities using the extensions in Sect. 4 to check the convex hulls that represent positional uncertainty, uncertainty in final turn radius, and uncertainty in the direction of travel.




(a) Evaluating alternatives (b) Uncertain position (c) Uncertain direction

**Fig. 4.** Practical extensions described in Sect. 4 allow us to safely evaluate turns initiated in the future that simultaneously have uncertainty in position and direction of travel. The modeled uncertainty can ensure that safety assessments are relevant despite wind, sensor error, and other deviations from the modeled kinematics.

This safety controller was integrated on a fixed-wing Swift Radioplanes Lynx aircraft (cruise speed 17 m/s) with an additional Raspberry Pi board. The controller operates as part of a larger message-passing system and subscribes to aircraft state messages published by the aircraft's autopilot (ArduPilot running on Pixhawk hardware). During normal operation, the aircraft is controlled by a primary controller. The fallback controller only intervenes when a predicted violation of the geofence is imminent. Upon a predicted violation of the geofence, the fallback controller issues a request to the ArduPilot autopilot to return to and then loiter around a known, safe waypoint. The parameters of the fallback controller were set according to our prior knowledge of the aircraft's roll rate and maximum (safe) turning rate used by the autopilot. We included one additional parameter not present in our theoretical model: the maximum round-trip time between receiving state information from the aircraft and executing the remediation. For our initial tests, we set this conservatively at 1 s.

Figure 5 plots the trajectories of the flight tests, showing rectangular geofence boundaries and a set of waypoints that the aircraft was asked to fly to sequentially. As the aircraft approached each waypoint, the safety controller would predict a future violation, take over, and override the autonomy by commanding a return to and loiter around the known safe waypoint in the interior. This implementation did not incorporate wind estimates, since they were unavailable at the time. Instead, we used a conservative estimate of worst-case wind effects to set model position uncertainty. We see that the wind, which blew primarily from the northeast that day, pushed the aircraft closer to the leftmost boundary, using up the margin of safety for the approach to the lower left waypoint in Flight Test 1.

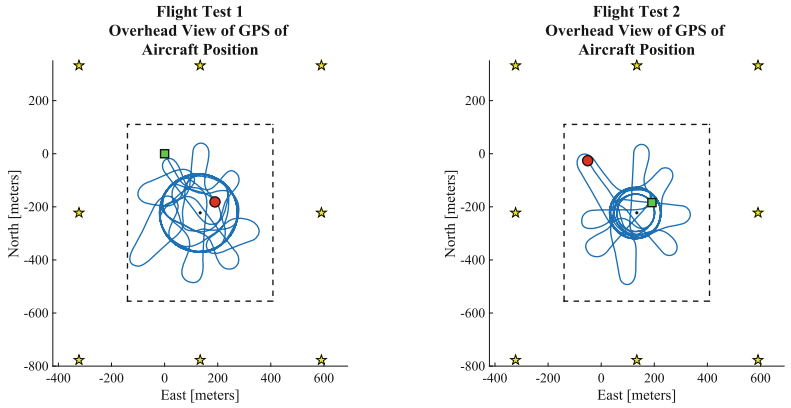



**Fig. 5.** Results of flight tests: Aircraft trajectories (in blue), from the start (green box) to the end (red circle), as the autonomy flies to each of the 8 commanded points (yellow stars) outside of the geofence. (Color figure online)

## 6 Conclusions and Future Work

We have extended predictive geofencing to turning models that increase the realism of predicted aircraft flight. The core of our approach has several desirable properties: the proofs of safety are formally verified and the computation of safety admits an efficient algorithm. We demonstrated the use of the predictive geofence safety theorem as a fallback controller, which was successfully flight-tested.

Future work regarding the formal proofs includes proofs of the extensions outlined in Sect. 4 to model uncertain parameter ranges and symmetry arguments that are currently associated with paper-only proofs.

Future work in integration and testing of these approaches includes further testing and calibration of the flight parameter ranges that serve as input to our algorithm. Initial testing of the predictive geofencing function was successful and further testing would enable wider adoption of this approach to verifying real-time safety controllers. In the long term, automatic extraction of the geofencing algorithm from the proofs would yield even higher assurances of correctness.

**Acknowledgements.** This work was supported by the US Air Force Research Laboratory's Strategic Development Planning and Experimentation Office under contract number HQ0034-19-D-0006. The authors would also like to thank Dr.'s Christopher Eaton, Edward White, and Reed Young for their leadership and fostering of this work. Additionally, we thank the entire team, especially Dorothy Kirlew and Andrea Jensenius, for their dedication in making the flight-testing of this approach possible.

## References

1. Brandse, J., Mulder, M., Van Paassen, M.M.: Clothoid-augmented trajectories for perspective flight-path displays. Int. J. Aviat. Psychol. **17**, 1–29 (2007)

2. Brezak, M., Petrović, I.: Path smoothing using clothoids for differential-drive mobile robots. In: Proceedings of the 18th World Congress the International Federation of Automatic Control, IFAC 2011, Milano, Italy, 28 August – 2 September 2011, vol. 18, pp. 1133–1138 (January 2011)
3. Cody, W.: Chebyshev approximations for the Fresnel integrals. Math. Comput. **22**(102), 450–453 (1968)
4. Dill, E.T., Young, S.D., Hayhurst, K.J.: SAFEGUARD: an assured safety net technology for UAS. In: 2016 IEEE/AIAA 35th Digital Avionics Systems Conference (DASC), pp. 1–10 (2016). https://doi.org/10.1109/DASC.2016.7778009
5. Gilabert, R.V., Dill, E.T., Hayhurst, K.J., Young, S.D.: SAFEGUARD: progress and test results for a reliable independent on-board safety net for UAS. In: 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), pp. 1–9 (2017). https://doi.org/10.1109/DASC.2017.8102087
6. Kikutis, R., Stankūnas, J., Rudinskas, D., Masiulionis, T.: Adaptation of Dubins paths for UAV ground obstacle avoidance when using a low cost on-board GNSS sensor. Sensors **17**, 2223 (2017)
7. Kouskoulas, Y., Renshaw, D., Platzer, A., Kazanzides, P.: Certifying the safe design of a virtual fixture control algorithm for a surgical robot. In: Belta, C., Ivancic, F. (eds.) Proceedings of the 16th International Conference on Hybrid Systems: Computation and Control, HSCC 2013, Philadelphia, PA, USA, 8–11 April 2013, pp. 263–272. ACM (2013). https://doi.org/10.1145/2461328.2461369
8. Kouskoulas, Y., Schmidt, A., Jeannin, J.B., Genin, D., Lopez, J.: Provably safe controller synthesis using safety proofs as building blocks. In: IEEE 7th International Conference on Software Engineering Research and Innovation, CONISOFT 2019, Mexico City, Mexico, 23–25 October 2019, pp. 26–35 (2019)
9. Levien, R.: The Euler spiral: a mathematical history. Technical report, UCB/EECS-2008-111, EECS Department, University of California, Berkeley (September 2008). http://www2.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-111.html
10. Lin, Y., Saripalli, S.: Path planning using 3d Dubins curve for unmanned aerial vehicles. In: 2014 International Conference on Unmanned Aircraft Systems (ICUAS), Orlando, FL, USA, pp. 296–304 (2014)
11. Loos, S.M., Renshaw, D.W., Platzer, A.: Formal verification of distributed aircraft controllers. In: Proceedings of the 16th International Conference on Hybrid Systems: Computation and Control, HSCC 2013, Philadelphia, PA, USA, 8–11 April 2013, pp. 125–130 (2013). https://doi.org/10.1145/2461328.2461350
12. Miraglia, G., Hook, L.: Dynamic geo-fence assurance and recovery for nonholonomic autonomous aerial vehicles. In: 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), St. Petersburg, FL, USA, pp. 1–7 (2017)
13. Monk, W.: Personal communication
14. Shanmugavel, M., Tsourdos, A., White, B., Żbikowski, R.: Co-operative path planning of multiple UAVs using Dubins paths with clothoid arcs. Control Eng. Pract. **18**(9), 1084–1092 (2010). https://doi.org/10.1016/j.conengprac.2009.02.010
15. Stevens, M.N., Rastgoftar, H., Atkins, E.M.: Specification and evaluation of geofence boundary violation detection algorithms. In: 2017 International Conference on Unmanned Aircraft Systems (ICUAS), Miami, FL, USA, pp. 1588–1596 (2017)
16. Team, P.: Px4 user guide: Geofence (2012). https://docs.px4.io/v1.10/en/flying/geofence.html. Accessed 7 Jan 2020
17. West, M.: Track transition curves (2012). http://dynref.engr.illinois.edu/avt.html. Accessed 7 Jan 2020

18. Wu, L., Zha, H., Xiu, C., He, Q.: Local path planning for intelligent vehicle obstacle avoidance based on Dubins curve and tentacle algorithm. In: SAE Technical Paper. SAE International (September 2017). https://doi.org/10.4271/2017-01-1951
19. Yoon, H., Chou, Y., Chen, X., Frew, E., Sankaranarayanan, S.: Predictive runtime monitoring for linear stochastic systems and applications to geofence enforcement for UAVs. In: Finkbeiner, B., Mariani, L. (eds.) RV 2019. LNCS, vol. 11757, pp. 349–367. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-32079-9_20