Integrity and Continuity for Automated Surface Conflict-Detection Monitoring

Mario, C. and Rife, J.;
Tufts Univ., Medford, MA, USA

This paper submitted to: IEEE Trans. on Intelligent Transportation Systems (submitted 2011)
Issue Date: TBA
Location: TBA
ISSN: TBA
Print ISBN: TBA
INSPEC Accession Number: TBA
Digital Object Identifier: TBA
Date of Current Version: October 25, 2011

This is a pre-print. Final Version available at <TBA>
Integrity and Continuity for Automated Surface Conflict-Detection Monitoring

Courtney Mario and Jason Rife, (Member, IEEE)

Abstract—This paper discusses how surface surveillance technologies impact the design of an automated conflict-detection capability for the Next Generation Air Transportation System, dubbed NextGen. In NextGen, automated Conflict Detection and Resolution (CD&R) algorithms will be necessary to assist air traffic controllers in identifying and mitigating potential hazards posed by non-conforming aircraft. Given this high reliance on automation, rigorous specifications for Conflict Detection (CD) algorithm continuity and integrity risk will be required. Continuity risk refers to the probability that a CD alert interrupts an ongoing operation; integrity risk refers to the probability that the CD algorithm fails to provide an alert rapidly enough to resolve the conflict. The continuity and integrity of CD algorithms depend strongly on the quality of surface surveillance sensor measurements; as such, we propose mechanisms for modifying CD&R algorithm design in order to account rigorously for the capabilities and limitations of surveillance sensors.

Index Terms—Air traffic control, alerting systems, conflict detection and resolution, surface traffic management

I. INTRODUCTION

Current estimates suggest that by 2018, NextGen traffic management will be able to reduce total delays by about 35% from forecast delays in the absence of NextGen. This reduction will provide an estimated $23 billion in total benefits to airlines, the public, and the FAA, and save about 1.4 billion gallons of fuel, cutting carbon dioxide emissions by about 14 million tons [1]. For the decade following 2018, these benefits should be either maintained or enhanced, even as the demand for air travel continues to grow. Airport operations are currently the primary bottleneck to improving the flow of air traffic over this timeframe. For this reason, new automation methods will be critical for streamlining surface traffic management, allowing for safe and efficient coordination despite an increased surface traffic density.

As one means for achieving this tight coordination, the NextGen work plan calls for the development of gate-to-gate Trajectory-Based Operations (TBO), in which aircraft would closely follow optimized, efficient trajectories [2]. Given the resulting high surface traffic density expected at major airports, as well as the expectation that trajectories will be automatically generated by computer algorithms, it is unrealistic to expect that ground controllers will be able to detect all possible conflicts that may arise if aircraft deviate from filed TBO flight plans. Therefore, automated Conflict Detection and Resolution (CD&R) algorithms will be needed to manage tactical separation assurance, enabling ground controllers to concentrate on traffic flow management at a strategic level.

The focus of this paper is to develop methods to embed sensor performance requirements directly into the function of surface CD&R algorithms that will support future TBO. Our work assumes a concept of operations in which computers will issue automated warnings and resolution orders directly to aircraft, resulting in a shift in responsibility towards automation and away from the current state of shared responsibility between human pilots and controllers. Moreover, we assume here that warnings and resolutions are issued by a ground system, and wirelessly communicated to aircraft, such that the alert system can leverage all available surveillance data (including surface radar and multilateration data, which may not be available to individual aircraft).

Surface CD&R algorithms are assumed to fulfill two functions: (1) detection of potential runway incursions, losses of separation, or other surface movement conflicts, and (2) generation of resolution orders that advise controllers and pilots how to achieve a safe outcome with minimal impact on surface traffic throughput. Though both functions are essential for safe and efficient TBO, this paper places particular emphasis on the Conflict Detection (CD) function.

Surface CD&R algorithms are somewhat different from airborne CD&R algorithms [3], in that the separation requirements for en route aircraft (typically 5 miles in the U.S. National Airspace) are much, much larger than the expected errors for navigation and surveillance sensors. In these cases, state-based [4] or intent-based planning [5] uncertainty typically dominates the overall uncertainty, although sensor errors may still play a role in tactical state-based conflict...
resolution [6]. By contrast, desired separation distances are significantly closer in value to sensor accuracy levels in surface CD&R.

In order to understand how surface surveillance systems will impact the performance of CD algorithms, it is important to quantify both the nominal operations and off-nominal behaviors of available surveillance sensors. Although a predictive CD algorithm might incorporate both velocity and position surveillance data, this paper will focus solely on position measurements, to establish a representative framework for embedding sensor performance requirements directly into CD algorithms. (The role of velocity data will be considered in future work.)

In the remainder of this paper we will describe a method to account specifically for nominal and off-nominal sensor behaviors in designing conflict detection algorithms. In the following section, we will first define two important performance metrics for characterizing a CD algorithm’s operational utility: continuity and integrity. In the next section, we will propose an example CD algorithm that inherently accounts for the continuity and integrity requirements. The remaining sections of the paper relate specific sensor technologies — such as radar, multilateration and ADS-B — to this example algorithm. A brief summary of our key points concludes the paper.

II. DEFINING CONTINUITY AND INTEGRITY

To be useful in an operational setting, the CD algorithm must at a minimum satisfy requirements for two essential performance metrics: continuity and integrity. Continuity is defined as the probability that a safety-critical operation is interrupted while in progress. Integrity is defined as the probability that an operation may be conducted under hazardous conditions without the knowledge of the pilot or air traffic controller (for instance, that an operation might be conducted based on faulty sensor data). Continuity and integrity metrics have been clearly defined in the navigation community [7]-[9]; however, while Required Navigation Performance has been well quantified by the FAA and other international civil aviation authorities (CAAs), Required Surveillance Performance (RSP) is still an emerging topic [10]-[12]. In this paper, we will adapt continuity and integrity definitions from the navigation industry [3]-[6],[13]-[17] to fit the scope of surveillance [18],[19].

An automated CD algorithm introduces a continuity risk in that planned operations may be aborted when the algorithm triggers an alert, indicating either a real or a perceived conflict between two taxiing aircraft or between an aircraft and a surface vehicle. As true conflicts are expected to be exceedingly rare, false alerts are expected to be the dominant source of continuity risk introduced by the CD algorithm. False alerts may occur either because of random sensor errors (also called Type I errors in statistical detection theory [20]) or because of sensor equipment failure. Both types of false alert will be considered in this paper, since they have similar impact on operations, degrading user confidence in the automated CD function and also introducing safety risk each time pilots are forced to react rapidly to a conflict resolution order.

By contrast, a loss of integrity occurs if an automated CD algorithm fails to trigger an alert in a timely fashion when a hazardous situation arises. Integrity loss might occur, for instance, if the CD algorithm is incomplete (algorithm not coded to recognize all possible conflicts) or if sensor data mask a potential hazard (due to equipment faults or large random errors). In this paper we assume the conflict detection algorithm is complete, such that integrity risk is primarily caused by random sensor errors (also called Type II errors in statistical detection theory [20]) or by sensor equipment failure.

To account for the many sources of continuity and integrity risk, a standard method from the risk analysis field is to employ fault trees [21],[22]. We assume that only a small fraction of the overall continuity and integrity risk budgets for surface movement is allocated to CD&R, and specifically to the impact of surveillance sensors on CD. As such, a major focus of this paper is to quantify how surface surveillance systems contribute to continuity and integrity risk, considering both nominal and off-nominal operating conditions. Nominal operating conditions refer to the surveillance systems’ typical performance and reported accuracies. Off-nominal operating conditions refer to circumstances where surveillance system function is suddenly and severely degraded. Two figures below illustrate the portions of the continuity (Fig. 1) and integrity (Fig. 2) risk trees associated with CD sensor performance. As shown in Fig. 1, the continuity budget is divided into the continuity allocation for nominal random noise, $C_{NR}$, and the continuity allocation for off-nominal events, $C_{OE}$. Similarly, as shown in Fig. 2, the integrity budget is divided into the integrity allocation for nominal random noise, $I_{NR}$, and the integrity allocation for undetected off-nominal events, $I_{UOE}$.

![Fig. 1. CD Continuity Risk Allocation for Surveillance Sensing.](image1)

![Fig. 2. CD Integrity Risk Allocation for Surveillance Sensing.](image2)
The following sections describe an approach for quantifying CD continuity and integrity risks. Particular attention is given to accounting for rare sensor errors that cause continuity loss due to a false alarm (Type I error) or integrity loss due to a missed detections (Type II errors).

In subsequent discussion, continuity risk due to rare nominal errors is quantified in terms of two related parameters: the continuity risk specification $C_{NR}$ and the monitor threshold $U$. The threshold $U$ is a bound on the sensor noise level under fault-free conditions. To prevent overly frequent alerts, the threshold must be set to be sufficiently wide to ensure that the continuity risk requirement is met, given the noise level of available sensor measurements.

In subsequent discussion, the integrity risk due to rare nominal errors is quantified in terms of three parameters: an operation-related risk specification $I_{NR}$, an alert limit $T$, and a time-to-alert $TTA$. For the case of a conflict due to a loss of separation, the alert limit is a bound on how close the measured separation approaches the separation minimum, given the uncertainty inherent in the surveillance sensor measurements. The FAA requires that any catastrophic event be extremely improbable, with an integrity risk below $10^{-9}$ per measurement. The time-to-alert is a bound on the required time-to-alert $TTA$.

Target values for the five continuity and integrity parameters (continuity threshold, integrity alert limit, continuity and integrity risk specifications, and time-to-alert) have not yet been established for the CD&R application; however, these values should be compatible with other planned and existing surface movement systems, such as the Advanced Surface Movement Guidance and Control System (A-SMGCS). Surveillance requirements for A-SMGCS surveillance in the movement area, under limited visibility conditions down to Runway Visual Range (RVR) of 75 m, are $2 \times 10^{-2}$/hour for system continuity and $2 \times 10^{-5}$/hour for system integrity (with a 10 second time-to-alert and a proposed 15 m horizontal alert limit) [18]. The implied threshold (based on a minimum one-sigma horizontal accuracy of 4 m) is approximately 12 m. Requirements in zero visibility conditions would likely be somewhat more strict, with system requirements on the order of $2 \times 10^{-2}$/hour for continuity and $10^{-9}$/hour for integrity. In theory, CD&R algorithms could be implemented as a sub-component of A-SMGCS. In this case, a fraction of the total continuity and integrity budgets for A-SMGCS would be sub-allocated to the CD&R function.

III. INTEGRATING CONTINUITY AND INTEGRITY INTO CD ALGORITHM DESIGN

A. Accounting for Nominal Errors

This section considers a specific implementation of a CD algorithm, for detection of conflicts between two aircraft occupying the same runway, and refines the algorithm to account specifically for continuity and integrity requirements. An example of a scenario in which a loss of separation might occur is when an aircraft merges onto a taxiway or runway occupied by a second aircraft, as illustrated in Fig. 3. In detecting conflicts between two aircraft occupying the same runway, it is assumed that trajectories are automatically generated for each aircraft, along with acceptable bounds for deviations by the pilot away from the nominal trajectory, in such a manner that all bounded trajectories are conflict-free. In other word, each trajectory is assumed to define a four-dimensional, space-time “bubble” in which the aircraft must remain. The nearest distance between these “bubbles” at any instant is assumed to define the required separation distance $S$ between aircraft at that instant.

If the CD algorithm determines that the aircraft pair has strayed closer than the time-varying separation requirement, an alert is triggered and the CD&R algorithm initiates conflict resolution. Because nominal aircraft trajectories are defined a priori in NextGen, the proposed resolution strategy covers both current and future conflicts. In effect, the future motion of the aircraft is encoded in the nominal trajectories, which in turn define $S$ as a function of time. This concept inherently differs from the state-of-the-art in other transportation applications (such as in the automotive arena [24]-[26]) where information about the future intent of nearby vehicles is not always assumed to be well characterized and bounded.

In order to account for continuity and integrity requirements as defined in the preceding section, we must account for the five continuity and integrity parameters. We propose that the CD algorithm should explicitly incorporate the continuity threshold and integrity alert limit parameters in monitoring aircraft separation. The allowed continuity and integrity risk specifications are interpreted as a means to assess whether or not available surveillance sensors comply with the specified alert limit and threshold. In this paper, we assume that surveillance sensors meet time-to-alert requirements, but this assumption could be relaxed in future research [23].

As a starting point, we identify two distinct separation requirements between aircraft: the minimum required separation $S_{min}$, which accounts for sensor uncertainty, and the noise-free minimum separation $S$, which is the time-varying required separation in the absence of sensor measurement errors. The quantity $S$ is a minimum separation that depends only on the type of operations being conducted, and not on the installed sensor surveillance equipment. Rather, the magnitude of $S$ is set to account only for physical
separation requirements and for imperfect tracking of the nominal trajectory by the pilot. To account for surveillance sensor uncertainty, the nominal separation \( S \) must be replaced with a larger value \( S_{\text{tot req}} \), which is the stricter reference separation which a pilot must maintain, accounting for surveillance sensor noise. In this sense, \( S_{\text{tot req}} \) is a critical parameter for generating conflict resolution orders (as well as for generating baseline 4D trajectories).

In addition to these two separation distances (noise-free \( S \) and total required \( S_{\text{tot req}} \)), a third distance is also critical: an intermediate distance at which the CD monitor will trigger, at some point between \( S \) and \( S_{\text{tot req}} \). This CD threshold point will be identified as being greater than \( S \) by a distance \( T \) and less than \( S_{\text{tot req}} \) by a distance \( U \), as shown in Fig. 4. Thus,

\[
S_{\text{tot req}} = S + T + U.
\]

(1)

For these parameters, the distance \( T \) is the integrity alert limit and the distance \( U \) is the continuity threshold. In the remainder of this section, we will derive probabilistic requirements that relate the definition of \( T \) and \( U \) to sensor performance.

The actual separation between an aircraft pair will generally be somewhat larger than the minimum requirement given by \( S \). We define the actual separation between aircraft to be \( S_{\text{true}} \). The following condition implies sufficient separation to ensure safe operations.

\[
\text{separation condition: } S_{\text{true}} \geq S
\]

(2)

Of course the CD algorithm is not aware of the true separation distance between aircraft, as sensor measurements are inherently noisy. Therefore, the measured separation distance between aircraft \( S_{\text{meas}} \) is perturbed from the true separation \( S_{\text{true}} \) accounting for a random sensor error \( \varepsilon \).

\[
S_{\text{meas}} = S_{\text{true}} + \varepsilon
\]

(3)

Maintaining a nominal separation of \( S_{\text{tot req}} \) between aircraft introduces a margin to ensure that the safety requirement (2) is met, even in the presence of sensor noise. It is the job of the CD algorithm to verify (2). To do this, the CD algorithm computes a monitor statistic \( m \).

\[
m = S_{\text{tot req}} - S_{\text{meas}}
\]

(4)

The monitor statistic is defined to be positive when surveillance sensors detect a loss of separation. Hence the CD algorithm should trigger an alert if the loss of separation grows too large. However, the alert should not be issued simply if \( m \) becomes positive, since, in the instance where the (noisy) measured separation \( S_{\text{meas}} \) is precisely at the allowed minimum of \( S_{\text{tot req}} \), there would be a 50% chance that the alert would be triggered falsely. Rather, the monitor should trigger at a threshold sufficiently large to limit the probability of false alarms. This operational consideration can be related to the continuity requirement; the alert should trigger if the loss of separation ever exceeds the continuity threshold.

\[
\text{alert condition: } m > U
\]

(5)

The probability of a false alarm \( P_{FA} \) is directly related to the distribution of errors \( \varepsilon \) for a given sensor and to the continuity threshold \( U \). Specifically, \( P_{FA} \) is the conditional probability that the monitor statistic exceeds the threshold given that the true aircraft separation is satisfactory, meaning that the true separation is greater than the total required separation.

\[
P_{FA} = P\{m > U \mid S_{\text{true}} - S_{\text{tot req}} \geq 0\}
\]

(6)

Because the continuity requirement must be satisfied for all allowable values of true separation, it is possible to replace (6) with a conservative form that considers only the worst-case allowed true separation. For a unimodal, zero-mean error distribution, the worst case separation, which results in the highest possible value of \( P_{FA} \), occurs when the true separation is a minimum, when \( S_{\text{true}} - S_{\text{tot req}} = 0 \). Using this limiting case in order to simplify (6), we obtain the following:

\[
P_{FA} \leq P\{m > U \mid S_{\text{true}} = S_{\text{tot req}} \}
\]

(7)

As long as sensor errors are sufficiently low that the expression on the right side of (7) does not exceed the continuity allocation for nominal random noise \( C_{NR} \), then continuity is assured independent of the true value of aircraft separation.

\[
\text{continuity requirement: } P_{FA} \leq C_{NR}
\]

(8)

Whether or not this requirement can be satisfied depends on the choice of the threshold \( U \) and the exact set of surveillance sensors used at the airport facility (see next section).

To help visualize this continuity requirement, the probability distribution for sensor error is illustrated in Fig. 5 for the worst-case conforming scenario, where \( S_{\text{true}} = S_{\text{tot req}} \). For the purposes of the illustration, the sensor error distribution, \( p(\varepsilon) \), is depicted as a Gaussian density function. The integrated probability over the shaded region of the density function is \( P_{FA} \), which represents the total probability.
probability that the error magnitude exceeds the threshold $U$ (in the direction of a false alarm).

Our CD algorithm design should also take into account integrity risk requirements. To meet integrity requirements, the probability that the safety criterion (2) is violated must be exceedingly small. In the absence of sensor noise, the safety criterion would always be met because the alert would be triggered at $S_{\text{true}} = S + T$, whereas a violation would only occur if $S_{\text{true}}$ were to become smaller than $S$. The margin provided by $T$ is essential to account for sensor errors, however. A sufficiently large sensor error could cause a missed detection event, in which the CD algorithm assesses an otherwise unsafe situation as safe. To meet integrity requirements, the missed detection probability $P_{MD}$ must be smaller than the integrity allocation for nominal random errors $I_{NR}$.

$$P_{MD} \leq I_{NR} \quad (9)$$

The probability of a missed detection $P_{MD}$ is directly related to the distribution of errors $\epsilon$ for a given sensor and to the alert limit $T$. Specifically, $P_{MD}$ is the conditional probability that the monitor statistic does not exceed the threshold given that the true aircraft separation is unsafe, meaning that the true separation is smaller than the minimum separation in the absence of a sensor error.

$$P_{MD} = P\{m < U \mid S_{\text{true}} - S < 0\} \quad (10)$$

Because the integrity requirement (9) must be satisfied for all unsafe values of true separation, it is possible to replace (10) with a conservative form that considers only the least-detectable case of a separation violation. For a unimodal, zero-mean error distribution, the least-detectable separation violation occurs when $S_{\text{true}} = S$. Using this limiting case in order to simplify (10), we obtain the following:

$$P_{MD} \leq P\{m < U \mid S_{\text{true}} = S\}. \quad (11)$$

As long as sensors errors are sufficiently low that the expression on the right side does not exceed the integrity allocation $I_{NR}$, then integrity is assured independent of the true value of aircraft separation. To help visualize this integrity requirement, the probability distribution for sensor error is shown in Fig. 6 for the least-detectable unsafe scenario, where $S_{\text{true}} = S$. In the figure, the $P_{MD}$ is the integrated probability over the shaded region of the density function, which represents the total probability that the measured separation is perceived to be safe (loss of separation less than $U$) given that the actual separation is insufficient.

The salient feature of our proposed CD algorithm design is the significant margin defined between the unsafe state ($S_{\text{true}} < S$) and the desired conforming state ($S_{\text{true}} > S_{\text{tot_req}}$). The intermediate region ($S_{\text{tot_req}} > S_{\text{true}} > S$) is a “gray area,” which is neither conforming nor unsafe. The defining characteristic of this region is that continuity and integrity requirements cannot be met within it. In other words, the monitor statistic noise is sufficiently large that the probabilities of a false alarm or of a missed detection occurring in this region are too high to support surface movement operations. The clear implication of the proposed approach is that the aircraft must maintain a somewhat larger minimum separation ($S_{\text{tot_req}}$) than the safety minimum in the absence of sensor error ($S$) such that the monitor threshold can be placed at an appropriate location between the two. A corollary is that high quality sensors are needed to permit dense aircraft spacing.

### B. Accounting for Off-Nominal Events

Surveillance sensor performance can be divided into nominal and off-nominal conditions. Nominal performance refers to cases in which the surveillance sensors are operating as intended. The probability density function defined in the previous section (to set $U$ and $T$) was assumed to describe sensor errors under nominal conditions.

Off-nominal conditions refer to any non-ideal situation in which the sensor fails to operate as intended. Because off-nominal events are rare exceptions, it can be challenging to model these events in any formal sense. Therefore, a conservative alternative is to model all off-nominal events simply as faults that may cause either a loss of continuity, integrity, or both [27],[28].

For continuity in this case, the total continuity budget for the CD algorithm $C_{CD}$ is split between two sub-allocations, one for nominal random events $C_{NR}$ and one for off-nominal events $C_{OE}$ (see Fig. 1):

$$C_{CD} = C_{NR} + C_{OE}. \quad (12)$$
The consequences of this decomposition of nominal and off-nominal events are two-fold. First, the fraction of the continuity risk budget available to $C_{NR}$ to bound nominal errors, according to (8), is reduced, placing a somewhat increased demand on sensor accuracy. Second, the probability of all off-nominal events must be summed, and the total probability must be shown to be smaller than $C_{DE}$.

Similarly, the total integrity budget for the CD algorithm, $I_{CD}$, must be split between allocations to cover nominal random errors, $I_{NR}$, and undetected off-nominal events, $I_{UOE}$ (see Fig. 2):

$$I_{CD} = I_{NR} + I_{UOE}.$$  (13)

It is important to note that only undetected off-nominal events count against the integrity budget. Some off-nominal events can be detected, and therefore those cases of faulty sensor measurements would be excluded from the CD algorithm. Specific mechanisms to implement such a fault-exclusion logic are not considered in this paper.

As in the continuity risk case, the consequences of decomposing the nominal and off-nominal integrity risk allocations are two-fold. Again, only a fraction of the total integrity budget is available for bounding nominal errors, according to (9). Additionally, the total probability of all undetected off-nominal events must be summed. In order for integrity requirements to be met, this total probability must be shown to be smaller than the allowed risk $I_{UOE}$.

One way to account for the summed risks of each of the off-nominal events is to use fault-tree analysis. A framework for fault-tree analysis for surface surveillance sensors is described in [28]. A full fault-tree, based on a Failure Modes and Effects Analysis (FMEA) to identify and quantify risk, is beyond the scope of our research. As such, off-nominal events will only be modeled coarsely in this paper (see Section V).

IV. SURVEY OF SURVEILLANCE SENSORS

An analysis of airport surveillance sensors is required to assess whether or not a particular CD algorithm can meet its continuity and integrity requirements. In this section, we will provide a brief overview of airport surveillance sensors in use or planned for deployment in the near future. The details of specific sensor technologies influence how their nominal and off-nominal errors are mapped into continuity and integrity requirements.

Relevant surveillance systems for detecting aircraft on the airport surface include radar, multilateration, and ADS-B. Radar technology has been around since the 1940s while more recently, multilateration systems have been approved for airport use since 2003 [29]. ADS-B is an emerging surveillance system in the process of being implemented and scheduled for complete implementation by 2020 [30]. This system uses positioning information, typically provided by onboard GPS. The integrity of this GPS sensing capability can be established through Receiver Autonomous Integrity Monitoring (RAIM), the Wide Area Augmentation System (WAAS), or, in the near future, the Ground Based Augmentation Systems (GBAS), which is scheduled to be fully operational sometime after 2016 [1],[31]. Camera-based visual surveillance systems are also under development [32],[33]; as these systems are in early stages of development and certification, they are not modeled in this paper.

A. Nominal Performance

Nominal performance is typically described by the accuracy of the reported position (and in a more general CD algorithm, by the accuracy of velocity information), as well as the frequency at which this information is reported. In general, accuracy is the nominal scatter of navigation errors, which for many sensors, is well described by a Gaussian distribution, at least near the distribution core [34]. Accordingly, sensor accuracy is often specified as a Gaussian sigma value that describes the distribution’s standard deviation. Typically, non-Gaussian tail behavior need only be considered in computing the false alert and missed detection probabilities (Fig. 5 and Fig. 6, respectively) if the alert limit $T$ and continuity threshold $U$ are much larger than 2-3 times sigma. In this work we will introduce an “inflation factor” of $\xi = 1.5$ to account for far tail (non-Gaussian) effects in using a Gaussian distribution. The 50% excess inflation value is approximate but representative for other applications [35]-[37]. Further work would be needed to validate this number for any particular sensor system operating at any particular airport facility [40].

It is convenient to characterize the error distributions for airport surface surveillance systems roughly in terms of 95% accuracy. The 95% accuracy corresponds to a 2-sigma value for a Gaussian distribution model. Nominal position and velocity measurement error for surface radar, multilateration, and ADS-B are summarized in Table I. These accuracy numbers are obtained from requirements documents and/or field assessments for each system [41]-[45]. The results shown in this table can be used to determine the appropriate continuity and integrity allocations for nominal random noise, $C_{NR}$ and $I_{NR}$, defined in the previous section and Fig. 1 and Fig.

<table>
<thead>
<tr>
<th>Surveillance System</th>
<th>Position Accuracy</th>
<th>Velocity Accuracy</th>
<th>Update Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radar</td>
<td>2 m</td>
<td>1 m/s</td>
<td>1 Hz</td>
</tr>
<tr>
<td>Multilateration</td>
<td>6 m</td>
<td>0.25 m/s</td>
<td>1 Hz</td>
</tr>
<tr>
<td>ADS-B (w/ SBAS)</td>
<td>2 m</td>
<td>0.1 m/s</td>
<td>1 Hz (0.2 Hz if stopped)</td>
</tr>
<tr>
<td>ADS-B (w/ GBAS)</td>
<td>1 m</td>
<td>0.1 m/s</td>
<td>1 Hz (0.2 Hz if stopped)</td>
</tr>
</tbody>
</table>
2. Similarly, for defined continuity and integrity budgets, these values can also be used to determine appropriate values for the continuity threshold, $U$, and integrity alert limit, $T$.

For large airport facilities, more than one of these sensing systems is available (or will be) to a sensor fusion processor. Surface surveillance data at major airports in the United States is currently compiled by the Airport Surface Detection Equipment – Model X (ASDE-X), a system produced by Sensis to integrate available sensor data for display to air traffic controllers [46]. The fusion process can improve the overall accuracy of the combined surveillance data; however, we will not explicitly model sensor fusion effects in this paper.

B. Off-nominal Performance

Off-nominal performance refers to conditions that can interrupt a sensor’s normal function. These occurrences are not well characterized by published accuracy information. In the most extreme cases, off-nominal behavior could result from an unrecoverable hardware failure (continuity loss) or from a partial hardware failure that causes a sensor to produce hazardous misleading information (integrity loss). Other events may be somewhat more common and somewhat less hazardous, such as a one-time sensor transmission or reception error. When considering all possible off-nominal events, it is important to realize that some events will impact both continuity and integrity requirements, while others may only impact one of these two.

Table II shows a list of the off-nominal events associated with each surveillance system. Further detail regarding all three systems as well as the associated off-nominal events is provided in [28].

The off-nominal performance associated with each of these systems can be used to determine the appropriate budgets for $C_{OE}$ and $I_{OES}$, represented in Fig. 1 and Fig. 2 as well as equations (12) and (13). A full quantification of the associated continuity and integrity impact of each of the above fault modes is beyond the scope of this paper. As such, we suggest that half of the overall continuity and integrity budgets be allocated to these off-nominal conditions, which is roughly consistent with the approach used in recent navigation system developments [21].

V. MINIMUM REQUIREMENTS FOR THRESHOLD AND ALERT LIMIT BASED ON SENSOR CAPABILITIES

This section provides estimates of the size of the alert limit $T$ and threshold $U$ based on sensor performance models, as described in the previous section. It is important to note that this paper’s main contribution is the method of integrating continuity and integrity requirements into a CD algorithm, and that future research will focus on obtaining more accurate estimates for all inputs used in this method. The numerical results obtained in this section are based on several simplifying assumptions, but they provide the framework to show how surface surveillance sensors impact CD algorithms.

For the purposes of making a rough estimate of $U$ and $T$, we will use the nominal accuracies described in Table I and make several supporting assumptions. Importantly, we assume that the surveillance sensor errors are zero-mean Gaussian and independent for each aircraft. In this case, the separation error (a difference of two Gaussian random variables) has a magnitude $\sqrt{2}$ times as large as the error magnitude for sensing each individual aircraft position. Rather than model the sensor fusion process in detail, we conservatively estimate that the accuracy of the fused position estimate is no better than the accuracy of the best available sensor (as characterized by Table I). Noting that the Gaussian sigma value is approximately half the 95% accuracy, while also accounting for the $\sqrt{2}$ factor mentioned above and the inflation factor $\xi$ to account for far-tail non-Gaussian behavior of the actual sensor error distributions, the error for the measured separation $S_m$ is $\sigma_s = \left(\frac{\xi}{\sqrt{2}}\right)\sigma_{table}$, where $\sigma_{table}$ is the entry in Table I associated with the most accurate available sensor technology.

This error model for $S_m$ feeds into computation of the probabilities of a false alarm or missed detection due to nominal random noise, according to (7) and (11). According to (8) and (9), the false alarm probability $P_{FA}$ can at most be equal to the continuity allocation $C_{NR}$, and the missed detection probability $P_{MD}$ can at most be equal to the integrity allocation $I_{NR}$. These limiting values of $P_{FA}$ and $P_{MD}$ result in the minimum possible (most favorable) values for $U$ and $T$. By evaluating (7) and (11) at these limits we obtain the following equations for $U$ and $T$.

---

**TABLE II**

Surveillance Sensor Off-Nominal Events

<table>
<thead>
<tr>
<th>Surveillance System</th>
<th>Off-Nominal Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radar</td>
<td>Signal Occlusion, Tracking Error, Rain and Ground Clutter Interference, Plot Extraction Error, Radar Tower Failure</td>
</tr>
<tr>
<td>Multilateration</td>
<td>Transponder Location Bias, Missed Message Error, Aircraft Transceiver Error, Ground Equipment Failure, Signal Spoofing, Signal Jamming, Message Collision, Ground Clock Synchronization Error</td>
</tr>
<tr>
<td>ADS-B</td>
<td>Improper Time Tagging, Missed Message, Aircraft Transceiver Error, Ground Equipment Failure, Signal Spoofing, Signal Jamming, Message Collision, GPS Fault</td>
</tr>
</tbody>
</table>
\[ U = -Q^{-1}(C_{\text{NR}}) \cdot \sigma_e \]  
\[ T = -Q^{-1}(I_{\text{NR}}) \cdot \sigma_e \]

Here \( Q \) is the Gaussian cumulative density function (CDF) for a unity-variance, zero-mean distribution, and \( \sigma_e \) is accuracy of the available sensor.

In order to evaluate these equations, values for both nominal continuity and integrity risks, \( C_{\text{NR}} \) and \( I_{\text{NR}} \), are required. The continuity and integrity specifications described in section II, \( 2 \cdot 10^{-5} \) hour for system continuity risk and \( 10^{-9} \) hour for system integrity risk, provide representative values for the requirements of an automated CD algorithm that supports NextGen operations. These requirements are given on a "per hour" basis, and so must be related to the probabilities of a missed detection or a false alert occurring at any particular instant in time. To relate per-hour specifications to the values of \( C_{\text{NR}} \) and \( I_{\text{NR}} \) used in (14) and (15), we assume the following.

First, we assume that fused sensor errors are highly correlated over the course of any operation with significant risk (such as landing, taking-off, merging, or crossing an active runway). If error values are correlated over an operation, then we can consider missed detection and false alarm probabilities on a per operation basis rather than on a per time-step basis. In fact, the correlation time constant for sensor errors is typically on the order of one to two minutes due to a combination of physics (e.g. correlated multipath errors) and measurement smoothing (e.g. low-pass filtering already applied to obtain the accuracies reported in Table I). Therefore it is both conservative and still representative to model continuity or integrity risk for an entire operation using the probability density function for the instantaneous sensor error at the moment that the loss-of-separation event occurs.

Second, we assume that for a high capacity airport there are 60 operations per hour in which aircraft separation approaches close to the minimum (and in which the monitor might flag, either as a false or true alarm). Dividing the total integrity and continuity budget per hour by 60 operations/hour gives the following values for the total continuity and integrity budgets for conflict detection, \( C_{\text{CD}} \) and \( I_{\text{CD}} \) respectively.

\[ C_{\text{CD}} = \frac{1}{60} \cdot 2 \cdot 10^{-5} \text{ / operation} \]  
\[ I_{\text{CD}} = \frac{1}{60} \cdot 10^{-9} \text{ / operation} \]

The total integrity and continuity allocations must be split between nominal and off-nominal events according to (12) and (13). In this light, we make one final important assumption: that \( C_{\text{OE}} \) and \( I_{\text{OUE}} \), continuity and integrity risks for off-nominal events, are allotted half of the overall total continuity and integrity risk budgets. With this, we obtain the following equation for the nominal continuity and integrity risk, \( C_{\text{NR}} \) and \( I_{\text{NR}} \).

\[ C_{\text{NR}} = 0.5 \cdot C_{\text{CD}} \]  
\[ I_{\text{NR}} = 0.5 \cdot I_{\text{CD}} \]

Combining these continuity and integrity allocations with the specifications in Table I, we are able to evaluate (14) and (15) to obtain a rough estimate of the threshold and alert limit, \( U \) and \( T \). These estimated values are summarized in Table III.

As mentioned earlier, it is important to note that the \( U \) and \( T \) values listed in Table III are based on a number of rough assumptions and approximations. In this light, the values in the table are intended to serve only as rough estimates and not as definitive values for design purposes. Although the tabulated values are only approximate, they do provide a sense of how nominal separation varies for different sensor configurations. It is clear that better surveillance sensors allow for more closely spaced aircraft, which can enable an increase in airport capacity. Ultimately, these rough calculations also provide an example of how our proposed mechanism for incorporating integrity and continuity risk into aircraft spacing requirement, which is the primary contribution of the paper, might be employed in practice.

VI. CONCLUSION

The key contribution in this paper is the development of a method of directly accounting for continuity and integrity risk in the definition of three key separation parameters for an automated surface CD&R algorithm. The three key separation distances are (1) the noise-free baseline separation, which is the separation that would be required if sensors were perfect; (2) the total required separation, which is the reference for pilot control actions and for definition of 4D trajectories and conflict resolutions; and (3) the monitor-threshold separation distance, at which the CD algorithm alerts pilots of a potential conflict and generates an automated resolution order. Furthermore, a clear relationship between enhanced surveillance sensor capabilities and denser aircraft spacing is shown, linking sensor performance with airport surface capacity. Because continuity and integrity are critical specifications for system certification, it is important that they should be considered even in the very earliest stages of CD&R algorithm design.
REFERENCES


Courtney Mario received her B.S. and M.S. degrees in mechanical engineering from Tufts University, Medford, MA in 2009 and 2011. As a graduate student, she worked as a research assistant in the Automated Systems and Robotics Laboratory at Tufts University. Her research has involved airport surface surveillance systems as well as automobile lane departure warning systems.

Jason Rife (M'01) received the B.S. degree in mechanical and aerospace engineering from Cornell University, Ithaca, NY, in 1996, and his M.S. and Ph.D. degrees in mechanical engineering from Stanford University, Stanford, CA, in 1999 and 2004. He is currently an Assistant Professor of Mechanical Engineering at Tufts University in Medford, Massachusetts. At Tufts, he directs the Automated Systems and Robotics Laboratory (ASAR), which applies theory and experiment to characterize the integrity of autonomous vehicle systems. Previously, after completion of his graduate studies, he worked as a researcher with the Stanford University GPS Laboratory, serving with the Local Area Augmentation System (LAAS) and Joint Precision Approach and Landing System (JPALS) teams.