An overview of GBAS integrity monitoring with a focus on ionospheric spatial anomalies

Sam Pullen & Per Enge
Department of Aeronautics and Astronautics, Stanford University, USA
E-mail: spullen@stanford.edu

Received 2 April 2007; accepted 14 May 2007

The Local Area Augmentation System (LAAS) or, more generally, the Ground Based Augmentation System (GBAS), has been developed over the past decade to meet the accuracy, integrity, continuity and availability needs of civil aviation users. The GBAS utilizes a single reference station (with multiple GNSS receivers and antennas) within an airport and provides differential corrections via VHF data broadcast (VDB) within a 50-km region around that airport. This paper provides an overview of GBAS integrity verification, explaining how integrity risk is allocated to various potential safety threats and how monitors are used to meet these allocations. In order to illustrate GBAS integrity monitoring in detail, this paper examines the potential threat of ionospheric spatial anomalies (e.g., during ionospheric “storms”) to GBAS and how GBAS protects users against this threat. In practice, the need to mitigate potential ionospheric anomalies is what dictates CAT I GBAS availability.

Keywords: LAAS, GBAS, Ionospheric spatial anomalies, Civil aviation
PACS No: 94.20.Vv; 94.20B6

1 Introduction

When the GPS standard positioning service (SPS), based on L1 C/A code, reached initial operational capability (IOC) in 1993, it was understood that SPS by itself could not meet the accuracy, integrity and continuity requirements of civil aviation users. At that time, SPS was intentionally degraded by selective availability (S/A), which made SPS ranging accuracy insufficient for precision-approach applications. In addition, while the GPS operational control segment (OCS) does its best to maintain the performance of GPS, it does not have the mandate to prevent or detect failures at the levels required for civil aviation operations. Receiver Autonomous Integrity Monitoring (RAIM) was developed to utilize satellite redundancy to enhance user integrity, but for a variety of reasons, it cannot be the sole means of providing integrity for civil aviation.

The use of differential GPS (DGPS) was originally developed as a means of defeating S/A and achieving metre-level accuracy. The Local Area Augmentation System (LAAS) was developed from generic local-area DGPS as a means to provide higher-accuracy differential corrections and integrity alerts via a radio data link. Early flight tests of prototype LAAS systems convincingly demonstrated the potential of this technology to replace and expand upon the capabilities of existing ground-based aircraft navigation aids such as VOR/DME and the Instrument Landing System (ILS). As a result, the International Civil Aviation Organization (ICAO) selected differentially-augmented GPS as the primary basis for future aircraft navigation and landing systems in 1995.

One of the key aspects of GBAS development was to determine as to how to protect users against GNSS or GBAS system failures that are rare but not so rare that they can be neglected. Several classes of potential failures in this category exist. Ranging source failures (e.g., failures within the GPS SPS) include:

(i) Excessive acceleration in GNSS ranging measurements (e.g., due to satellite clock failures),
(ii) GNSS navigation data failures (significantly erroneous clock and/or ephemeris data),
(iii) Code-carrier divergence in GNSS satellite range measurements,
(iv) Low GNSS satellite signal power,
(v) Deformation of GNSS code signals.

The primary failure mode within the GBAS ground system is the failure of a single ground receiver out of the four receivers typically fielded at a GBAS site. Two potential atmospheric-propagation anomalies exist, i.e. ionospheric and tropospheric ones. Finally,
RF interference occupies a category of its own, because it tends to be localized in impact, but is not part of GNSS or GBAS.

This paper describes the methods used by GBAS to mitigate these potential threats and briefly discusses how future upgrades to GBAS will allow for better mitigation of worst-case ionospheric impacts on user errors and thus provide higher availability.

2 Summary of civil aviation requirements

Requirements for civil aviation operations supported by GBAS were derived from the requirements that apply to existing navigation aids, such as ICAO Annex 10 for ILS. Detailed listings of these requirements can be found elsewhere. The key parameters upon which requirements are placed can be defined as follows:

Accuracy: Measure of navigation output deviation from truth, usually expressed as $1\sigma$ or 95% (approximately $2\sigma$) error limits.

Integrity: Ability of a system to provide timely warnings when the system is unsafe to use for navigation.

Integrity risk: It is the probability of an undetected (and potentially hazardous) navigation system state.

Continuity: Likelihood that the navigation signal-in-space supports the accuracy and integrity requirements for the duration of intended operation.

Continuity risk: It is the probability of a detected but unscheduled navigation interruption after the initiation of an approach.

Availability: Fraction of time navigation system usable (as determined by compliance with accuracy, integrity and continuity requirements) before approach is initiated.

These requirements are parametrized in such a way that each aircraft is able to determine, before beginning an operation, whether or not it can proceed. The aircraft does this by computing (i) position-domain ‘protection levels’, based on the GPS satellites in view and approved by GBAS, (ii) the ranging error standard deviations or ‘sigmas’ broadcast by GBAS and (iii) the ‘K-value’ multipliers needed to achieve the required integrity and continuity risk probabilities based on a zero-mean Gaussian distribution of nominal errors. For GBAS requirements, the integrity requirement dominates the accuracy requirement; thus verification of integrity also confirms accuracy. Continuity is covered by only including the set of measurements whose probability of remaining usable throughout an operation is below the continuity risk requirement for that operation. Details on these protection level calculations are covered in Sec. 4.

3 GBAS architecture overview and required fault monitors

The fundamental system element for both GBAS and SBAS is the reference station, comprising one or more reference receivers connected to antennas at fixed locations known (pre-surveyed) to within 1-2 cm. These reference receivers provide continuous measurements for all GPS satellites in view, so that differential corrections can be formed. They typically have multiple receivers and antennas to provide the required availability and continuity and to allow failures of individual reference receivers which can be detected and excluded before they corrupt the differential corrections. Approved corrections and error bounding sigmas (to support protection level calculations; see Sec. 4) are broadcast to users via the VHF data broadcast (VDB) at a 2-Hz rate.

Figure 1 shows a functional block diagram for the Stanford University LAAS ground facility (LGF) prototype known as the Integrity Monitor Testbed (IMT). The functions shown in yellow boxes are those required to calculate DGPS corrections. These algorithms are well understood and comprise perhaps 10% of the IMT software. The functions shown in green boxes are groupings of integrity monitor algorithms that are designed to detect different failure modes as follows:

SQM (Signal Quality Monitoring): Detects satellite signal deformation, low signal power and code-carrier divergence.

DQM (Data Quality Monitoring): Detects anomalies in satellite navigation data (ephemeris and clock data).

MQM (Measurement Quality Monitoring): Detects step, ramp and acceleration errors in reference receiver measurements (may be due to satellite or receiver faults).

MRCC (Multiple Receiver Consistency Check): Computes $B$-values that compare measurements across reference receivers and uses them to detect reference receiver failures.

$\sigma\mu$-monitor (Sigma-Mean Monitor): Collects $B$-values over time and uses them to detect violations of the broadcast pseudo-range correction error sigma ($\sigma_{pr,\text{gnd}}$) and assumed mean of zero.
The IMT implementation of these functions is elaborated elsewhere\textsuperscript{19,22}.

The remaining 30-40\% of the code is dedicated to Executive Monitoring (EXM), which collects the outputs from each monitor and determines which measurements, if any, are flawed and must be excluded from the set used to compute the differential corrections sent to users. The EXM in IMT is primarily based on Boolean logic.

For example, monitor alerts (generated when a test statistic exceeds its pre-set acceptability threshold) on multiple satellites tracked on a single reference receiver, and all measurements on that receiver are considered to be faulty unless more than one of the flagged satellites is also flagged on one of the other reference receivers. If this latter event occurs, no clear diagnosis of a reference receiver or satellite failure can be made, and IMT must temporarily shut down\textsuperscript{19} (in this case, broadcast empty correction messages, indicating that no satellites can be safely used).

4 GBAS integrity verification and mitigation of anomalies

Figure 2 shows as to how the total GBAS signal in space (SIS; encompassing the GPS satellites and GBAS VDB) integrity risk requirement of $2 \times 10^{-7}$ per approach is allocated. One-fourth of this total is split evenly between the nominal or fault-free (known as ‘H0’ in GBAS) hypothesis and the single-receiver fault (H1) hypothesis. The vertical protection level (VPL) for the H0 hypothesis is given in a simplified form\textsuperscript{13} by

\[
VPL_{H0} = K_{FFMD} \sigma_{vert,H0}
\]  

where $\sigma_{vert,H0}$ is derived by computing the weighted pseudo-inverse matrix $S$ based on the line-of-sight vectors to the satellites and the range error (after corrections are applied) sigmas broadcast for each approved satellite. A separate VPL for the H1 hypothesis is given by, in simplified form, as follows:

\[
VPL_{H1} = |B_{vert,H1}| + K_{MD} \sigma_{vert,H1}
\]  

Here, $B_{vert,H1}$ represents the vertical position domain impact of the largest possible bias error due to one reference receiver being failed. Because individual pseudo-range corrections for each reference receiver are computed before being averaged into a single correction for each satellite, the range-domain bias error under the assumption that any one of the three or four reference receivers has failed can be computed, and the maximum value for each reference receiver is broadcast by the VDB to users. As with the VPL$_{H0}$ in Eq. (1), users apply their known satellite geometry to compute the maximum $B$-value in the vertical error domain and apply the result in Eq. (2) (see Refs 10 and 19 for details). Note that $K_{MD}$ in Eq. (2) is lower.
than $K_{\text{FFMD}}$ in Eq. (1) because, while $K_{\text{FFMD}}$ must cover the entire integrity risk due to nominal conditions, $K_{\text{MD}}$ only needs to cover the residual risk given that a single-receiver fault has occurred. As a result, the total probability of any one reference receiver failing and creating H1 risk must be below $10^{-5}$ per approach\textsuperscript{10,12}.

One other thing to note is that, while $K_{\text{FFMD}}$ and $K_{\text{MD}}$ are based on zero-mean Gaussian distributions of pseudo-range errors, actual pseudo-range error distributions are non-Gaussian (and typically fatter than Gaussian) in the tails. Therefore, the broadcast range-domain error sigma, or $\sigma_{\text{pr,gnd}}$, must be inflated, so that the implicit Gaussian assumption of Eqs (1) and (2) covers the actual non-Gaussian risk in these tails. Since the ‘true’ error distribution cannot be determined with certainty, the best means to determine the amount of inflation requires an active area of research\textsuperscript{23,24}.

As shown in Fig. 2, the remaining 75% of the total integrity risk not allocated to the H0 and H1 hypothesis (or $1.5 \times 10^{-7}$ per approach), is allocated to all other fault or anomaly conditions including GPS satellite anomalies. Of these, the LAAS MASPS allocates $2.3 \times 10^{-8}$ per approach to single-satellite ephemeris failures. This specific allocation corresponds to the fixed $K$-value in the ephemeris VPL ($\text{VPL}_{\text{eph}}$) equation, which is also computed by users based on an uplinked $P$-value\textsuperscript{12,20,21}. The remaining integrity risk, $(1.5-0.23) \times 10^{-7} = 1.27 \times 10^{-7}$ per approach, is allocated to the remaining single-satellite failures and all other failure conditions by the GBAS ground system manufacturer (Fig.2 shows one example of allocation). These allocations need not be standardized, because no protection levels (requiring fixed $K$-values) are computed for them by users.

The protection levels computed by users (specifically, the maximum value obtained one each from $\text{VPL}_{\text{H0}}$ calculation, $\text{VPL}_{\text{H1}}$ calculation for each operating reference receiver, and $\text{VPL}_{\text{eph}}$ calculation for each satellite used for positioning) are compared to alert limits in each position axis of interest to determine if the system meets the integrity and continuity requirements for a given operation\textsuperscript{4,10,12}. These values are set on the basis of maximum safe excursions from nominal flight paths depending on the presence of nearby obstructions. Figure 3 shows how these alert limits decrease as the aircraft gets closer to the runway and to obstacles on the ground. Because GPS satellite geometries are least favourable in the vertical direction, and because obstacles are more threatening in the vertical direction, the vertical alert limit (VAL) is the driving requirement (i.e., meeting the VAL requirement for a given operation ensures that the corresponding HAL or LAL requirements are met practically in all cases).

The purpose of the integrity monitor algorithms described in Sec.3 is to detect and exclude faults and other anomalies before they become hazardous to users so that the nominal protection level given by $\text{VPL}_{\text{H0}}$ in Eq. (1) covers all the remaining error sources. However, in practice, this cannot be done perfectly. The detection thresholds for these monitors must be high enough to ensure that, under fault-free conditions, the threshold is very rarely violated (this is
to ensure that the continuity requirement is met). A fault whose mean impact on the test statistic is to push it to the threshold value, thus, will be detected with a probability of 0.5 (noise is equally likely to push the statistic above or below the threshold), which is insufficient. The error that will be detected with a missed-detection probability ($P_{MD}$) sufficiently low to meet the integrity risk requirement is one whose mean impact on the test statistic is known as the minimum detectable error (MDE) and is defined as

$$MDE = T + K_{MD} I_{test} \sigma_{test} \quad \ldots(3)$$

where $T$ is the detection threshold, $K_{MD}$ the $K$-value multiplier needed to give the required $P_{MD}$ from a one-sided zero-mean Gaussian distribution of unit variance, $\sigma_{test}$ the actual test statistic sample variance under nominal conditions and $I_{test}$ the inflation factor needed for the assumed zero-mean Gaussian distribution to bound the actual test statistic distribution at and beyond $P_{MD}$. Typically, the threshold $T$ is derived from

$$T = K_{FFD} I_{test} \sigma_{test} \quad \ldots(4)$$

where $K_{FFD}$ is analogous to $K_{MD}$, but is based on the allocated probability of fault-free detection from the continuity requirement. Thus, MDE can be simplified to:

$$MDE = (K_{FFD} + K_{MD}) I_{test} \sigma_{test} \quad \ldots(5)$$

Figure 4 shows a graphical illustration of the definition of the threshold and MDE for the typical case, in which, as done in Eqs (3)-(5), the nominal monitor test statistic is assumed to be zero-mean Gaussian and faults are modelled as adding fixed bias offsets to the nominal test statistic. Once MDE is obtained for a given threat, a worst-case error (WCE) in the range domain can be computed as an analog to the VPL$_{H1}$ and VPL$_{eph}$ fault-mode protection levels as follows:

$$WCE = E_{R,MDE} + K_{MD} \sigma_{fault} \quad \ldots(6)$$

where, $E_{R,MDE}$ is the range-domain error resulting from the fault magnitude indicated by MDE, and $\sigma_{fault}$
is the nominal range-domain error, sigma, given the assumed fault condition (in most cases, the only fault impact is the addition of the fixed bias error modelled by MDE, $\sigma_{\text{fault}}$ is typically the same as the nominal range-domain error sigma). Note that $K_{\text{MD}}$ in Eq. (6) is meant to represent the same gap between fault mode prior-probability and required integrity allocation as $K_{\text{MD}}$ in Eqs (3) and (5). Using of $K_{\text{MD}}$ twice is typically conservative, because it applies this “missed-detection” buffer to both the derivation of MDE in Eq.(5) and to the addition of nominal error in Eq. (6).

If WCE for each possible fault condition could be uplinked in the VDB, user protection levels for all such faults could be computed in the manner of H1 and ephemeris fault conditions [i.e., by converting both terms on the right-hand-side of Eq. (6) into position-domain bounds based on the known user satellite geometry][13]. It would be straightforward to determine the total integrity protection level for all conceivable faults at the aircraft. However, in practice, this is not possible because (a) all faults of concern do not fit the zero-mean-Gaussian-plus-fault-bias model of the above equations [Eqs (1)-(6)] and (b) even if (a) were not true, the definition of the ground-to-user Interface Control Document (ICD) that the VDB must support, occurred well before all the possible faults of concern were understood well enough to be modelled[17]. Therefore, as shown in Fig. 2, all faults in the "'H2' category (meaning all conditions that are not H0 and not H1), except for ephemeris failures, do not have user protection levels. This means that the GBAS ground station is responsible for protecting all possible user satellite geometries (i.e., subsets of the satellites for which pseudo-range corrections are broadcast). In addition, while comparing position-domain WCE values to alert limits they should be sufficient to demonstrate safety. Instead, GBAS standards generally require that these values be bounded by $\text{VPL}_{\text{H0}}$ from Eq.(1) as well[10,11].

To achieve these requirements for non-ephemeris H2 fault modes, several related methodologies have been proposed to connect MDE, WCE and $\text{VPL}_{\text{H0}}$. These methods are often described by the term MERR, which refers to the maximum error impact of a fault in the range domain that implicitly meets the VPL-bounding requirement for all possible user geometries. Note that MERR is different from MDE in the sense that MDE is computed in the test-statistic space, whereas MERR is derived in the pseudo-range-error space. In practice, what is normally done is to derive MDE for the selected integrity monitor algorithm, translate the fault magnitude implied by MDE into pseudo-range error $[\text{Eq}(\text{MDE})$ in Eq.(6)], and then compare the resulting error with an MERR value derived independently based on the definition of $\text{VPL}_{\text{H0}}$ and the integrity risk sub-allocation to the fault mode in question. The derivations given by Shively and Zaugg assume the worst theoretically-possible user geometry, which is the worst of all theoretical geometries that result in $\text{VPL}_{\text{H0}} \leq \text{VAL}$, and then express MERR in terms of a multiplier of $\sigma_{\text{pr, gnd}}$, which is the ground-system range-domain component of the nominal error sigma which results in the total (ground plus user) vertical error sigma $\sigma_{\text{vert, H0}}$ in Eq.(1) [see Refs 12,13 and 23].

Multiplier based on the methods given by Shively and Zaugg are typically in the range of 3-6. Since $\sigma_{\text{pr, gnd}}$ for CAT I GBAS is in the order of 0.1-0.25 m (Ref. 27); the required MERRs are quite small – typically less than 1 m. Somewhat less conservatism can be arrived at by simulating the actual GPS satellite orbits as seen by GBAS users and finding the largest possible $S_{\text{vert}}$ multiplier (the multiplier that translates range domain error to vertical position domain error[13]) that could be generated by an actual user subset geometry which meets the $\text{VPL}_{\text{H0}} \leq \text{VAL}$ constraint (this maximum value of $S_{\text{vert}}$ is about 5-6). A more-generalized approach to MERR derivation that includes time-to-alert can be found. This approach is more easily applied to integrity monitor design because it expressly accounts for monitor-test-statistic-step response to the onset of a failure and constrains monitor performance with the 6-second SIS time to alert for CAT I GBAS.

5 Threat of ionospheric spatial anomalies to GBAS

The ionosphere is a dispersive medium located in the region of the upper atmosphere between ~50 km and ~1000 km above the earth[30]. In the ionosphere, the sun’s radiation produces free electrons and ions that cause phase advance and group delay in radio waves. As GPS signals traverse the ionosphere, they are delayed by an amount proportional to the total electron content (TEC) within the ionosphere at a given time. Because the ionosphere is constantly changing, the error introduced by the ionosphere into the GPS signal is highly variable and is difficult to model at the level of precision needed for GBAS. However, under nominal conditions, the spatial gradient is in the range of 2-4 mm/km ($\sigma$); thus
typical GBAS user errors are small (less than 10 cm, 1σ, see Refs 27,31).

The possibility of extremely large ionospheric spatial gradients was originally discovered in the study of WAAS “supertututh” (post-processed, bias-corrected) data during ionosphere storm events at the time of last solar maximum (2000-2001). In particular, gradients over 100 mm/km were discovered in the north-east corner of the Conterminous U.S. (CONUS)32,33 on 6 Apr. 2000. Even several stronger ionospheric storms have occurred since the April 2000 storm, the two largest ones being during 29-31 Oct. 2003 and on 20 Nov. 2003. Figure 5 shows the change of ionospheric delay on one particular GPS satellite as viewed by several IGS/CORS reference stations in the Ohio/Michigan region34 on 20 Nov. 2003. The sharpest gradient observed to date is the very sharp fall-off of ionospheric delay just before 2100 Zulu on this date, while smaller but still anomalous gradients were observed as the ionospheric delay rose and then fluctuated between 1800 and 2045 Zulu. These large gradients cannot be bounded by five or six times the nominal σv (or “sigma vertical ionosphere gradient) of 2-4 mm/km cited above; thus they must be treated as anomalies.

In order to be able to simulate the impact of such large gradients on GBAS users, a simplified “linear wave front” model of large-scale ionospheric spatial anomalies was created34 as shown in Fig. 6. In addition to the gradient slope in mm/km, the key parameters are: (i) the width of the gradient (in km), (ii) the forward propagation speed of the “wave front” relative to the ground (in m/s), and (iii) the maximum difference (in m) in the ionospheric delay. While we can tell from post-processed WAAS and IGS/CORS data that actual structures of ionosphere are non-linear and do not propagate forward at a constant velocity, the data are too sparse, at present, to support a more intricate model.

The approach chosen to provide bounded ranges of numbers for each of the parameters in this model was to sort, through the existing post-processed L1-L2. ionospheric delay data for stormy ionosphere days in
CONUS, pick out structures with large apparent gradients and fit parameter estimates to them, and then cross-check the resulting parameter estimates with raw L1 code-minus-carrier measurements to eliminate apparent gradients that were actually due to loss of lock on semi-codeless L2 signals. Figure 7 illustrates this process. In practice, the vast majority of apparent large gradient observations (on days known to have large gradients) cannot be validated as being ‘true’ ionospheric gradients with sufficient confidence. As a result, the number of validated anomaly observations is in the order of tens out of hundreds of observations analyzed in detail.

Figure 8 summarizes the results of this analysis process by plotting validated observed anomalies in terms of estimated propagation speed as a function of gradient-slope (front width proved to be too hard to precisely estimate from ground stations, typically more than 50 km apart, but fortunately the worst-case GBAS user impact is not strongly dependent on width). These results provided the basis for the development of the GBAS ionospheric anomaly threat model, which provides parameter-bounds for each of the parameters in the linear wavefront model of Fig. 6. Since the impact of this anomaly on GBAS is driven by the point in this threat model that causes the largest GBAS user error (prior to GBAS ground station detection and exclusion) for the worst-case combination of aircraft precision approach parameters, this threat model was drawn to tightly bound the observed and validated anomaly points (and two-sigma error bars) as shown in Fig. 8.

Figure 9 shows the resulting threat model in terms of gradient vs ground speed for various satellite elevation angles. Note that, as in Fig. 8, the threat model expresses ionospheric gradients and differences in maximum delay in terms of slant (not zenith) delay. The ionospheric thin-shell model, which is used to convert zenith to slant delays based on a satellite-elevation-angle-dependent obliquity factor, is avoided wherever possible, because the thin-shell model of the ionosphere does not appear to model accurately the ionospheric storm conditions. However, the thin-shell model must be used to some degree, because the linear-wave-front threat model still assumes that
Also note that the width parameter (not shown in Figs 8 and 9) is allowed to vary between 25 and 200 km, while the maximum difference in ionospheric delay is 50 m (i.e., any set of parameters, otherwise inside, the threat model for which the product of slope and width exceeds 50 m is not included the threat model).

One important feature of Fig. 9 is that it shows as to how the maximum possible gradient varies with front speed and satellite elevation angle. The largest possible gradient, 330 mm/km, is only possible for front speeds greater than 375 m/s with respect to the ground. Gradient magnitude also decreases with elevation angle. The maximum gradient of 330 mm/km is only possible for elevation angles exceeding 30°. These relationships become important when IPP velocity is brought into the analysis, which is discussed in Sec. 6.

6 GBAS mitigation of ionospheric spatial anomaly threat

Using the wave-front model of Fig. 6 and the bounding anomaly parameters of Fig. 9, it is possible to simulate the impact of a specific ionospheric anomaly scenario on a GBAS user aircraft approaching a GBA-equipped airport. This simulation requires an algorithm to select the most severe combination of ionospheric anomaly parameters for a given satellite IPP. Note that the observed velocity of an ionospheric wavefront (modelled as shown in Fig. 6) at a given ground station IPP is the difference (or Δv) between the wavefront speed with respect to the ground and the speed of the IPP itself, which moves with the orbiting satellite that generates this (theoretical) IPP. As shown in Fig. 10, it is possible for speeds of 300 m/s or higher to exist for low-elevation satellites, which means that it is possible for fast moving (and thus potentially high-gradient) wavefronts to appear stationary to the GBAS ground station, because the wavefront motion is “cancelled out” by IPP motion in the same direction. Fortunately, if this occurs, the maximum gradient will still be constrained by the low elevation angle that makes such fast IPP speeds possible.

Ionospheric-gradient wavefronts that become visible to the GBAS ground station can be detected by the ground-station code-carrier divergence (CCD) monitor[^19]. This monitor has a minimum detectable error expressed in terms of apparent temporal gradient (in m/s) as observed by the fixed ground-station antennas. Thus, worst-case scenarios, from the point of view of a GBAS user approaching a GBAS-equipped airport, are cases in which the ionospheric wavefront is almost stationary with respect to the ground station or cases in which the wavefront approaches from “behind” an approaching aircraft and generates a very large differential range error at that aircraft just before the front impacts (and is soon detected by) the ground system CCD monitor[^34].

To evaluate worst-case user-position errors due to ionospheric anomalies, a standard simulation of GPS satellite geometries using the RTCA-standard 24-satellite constellation[^13] has been applied to three airport locations in CONUS, i.e. Memphis, Tennessee (the future site of the first operational GBAS Category I ground station in the U.S.) and Los Angeles, California. For a given location and time, this simulation applies to ionospheric anomalies modelled as shown in Fig. 6 on all independent combinations of two satellite IPPs. One IPP is subjected to the worst possible ionospheric anomaly wavefront based on prior simulation of worst-case range-domain errors (including the impact of ground system CCD monitoring) for the conditions relevant to that IPP, while the ionospheric impact on the second IPP (which is affected simultaneously) is directly computed from what was found to be worst for the first IPP. After deriving the worst-case vertical position error for that case, the scenario is repeated but with the ionospheric scenario determined by what is worst for the second IPP. The worst-case errors from this two-IPP simulation approach have been found to be somewhat worse than the worst-case error when only one IPP is impacted[^36].
Figure 11 shows (as an example) the result of this simulation approach for the Memphis airport location for a user at an approach-threshold of 5 km from the GBAS ground system over one repeatable day of GPS satellite geometries. Figure 11 plots MIEV, the maximum ionospheric error in vertical (position), for both all-in-view geometry (with all 24 satellites in the RTCA constellation assumed to be healthy) and the worst possible subset user geometry, which includes all independent combinations of four or more satellites from the all-in-view geometry that meet the \( \text{VPL} \leq \text{VAL} \) constraint. The MIEV is defined based on Eq. (6) converted into vertical position error with \( K_{MD} = 3.1 \). Thus, it is analogous to H1 and ephemeris VPLs defined for other fault conditions.

As shown in Fig. 11, MIEV for the all-in-view geometry is typically around 10 m (which is the standard FASVAL, or VAL at the threshold or decision height, for Category I precision approaches\(^{37}\), but is much larger than the un-inflated \( \text{VPL}_{40} \). The situation is much more severe when the worst possible subset geometry is considered, as MIEV, in that case, varies between 25 and 40 m. While the worst possible subset geometry is constrained beyond what is shown in Fig. 11 by the Bias Approach Monitor (BAM) check dictated by the LAAS MOPS\(^ {13,36} \), the worst-case MIEV, after BAM is taken into account, is still in the neighbourhood of 35 m.

Given this result, there is clearly no hope of MIEV being bounded by \( \text{VPL}_{40} \), and it is also impossible to bound MIEV with a 10-m FASVAL with acceptable availability. Fortunately, FAA studies of WAAS LPV approach applicability to the 200-ft decision height that applies to Category I precision approaches\(^ {37} \) suggest that a FASVAL of as large as 35 m is sufficiently safe for Category I approaches. Therefore, FAA is willing to consider the same FASVAL for the worst-case of ionospheric anomaly scenario as the sufficient mitigation. This allows one to define \( \text{FASVAL}_{H2} \) (or FASVAL for the H2 ionospheric anomaly scenario) to be 35 m (although the value of \( \text{VAL}_{H2} \) further away than the approach threshold, is yet to be determined). With this definition of \( \text{FASVAL}_{H2} \), it should be possible to provide 99.9% or higher availability for Category I precision approaches when all 24 primary-orbit-slot GPS satellites are healthy. This is because only moderate inflation of the broadcast \( \sigma_{pr_gnd} \) and \( \sigma_{vig} \) is required to make all otherwise feasible subset geometries with MIEV > \( \text{VAL}_{H2} \) unavailable by increasing \( \text{VPL}_{40} \) above the 10-m ‘normal’ FASVAL applied by the aircraft.

7 Summary and CAT II/III GBAS prospects

This paper has described as to how ground-based GNSS augmentation provides additional integrity to support aircraft precision approaches up to and including Category I precision approach. The key to GBAS integrity assessment is the definition of protection levels to express position error bounds at the defined integrity risk probabilities that are sub-allocated from the overall integrity risk requirement.
(2.0 × 10⁻⁷ per approach for Category I). These protection levels bound the rare-event errors due to nominal conditions (H0), single-reference-receiver fault conditions (H1) and ephemeris failure conditions (one component of H2). For these conditions, GBAS users compute protection levels in real-time and compare them to the defined alert limits for particular operations to obtain an indication as to whether or not the operation is safe. For fault conditions, not covered by specific user protection level equations, several conservative methods have been derived to relate integrity monitor performance with integrity risk sub-allocations based on the MERR concept.

As ionospheric spatial anomalies can create GBAS user errors that cannot be bounded by MERR or by nominal VPL, a unique mitigation approach has been developed for this class of anomalies. A threat model of possible ionospheric anomaly behaviour has been developed based on observed and validated ionospheric gradient anomalies discovered in WAAS and IGS/CORS data. User geometry and ionospheric wavefront simulation is used to find the worst-case impact of anomalies within the threat model on aircraft conducting GBAS precision approaches. This worst-case impact is compared to a vertical alert limit (used only for rare-event ionospheric anomalies) to determine if a given set of user geometries is safe. If not, inflation of the broadcast $\sigma_{\text{pr-gnd}}$ and/or $\sigma_{\text{vig}}$ is required to make possible unsafe subset geometries unavailable at the user (the sigma inflation must be sufficient to cause $\text{VPL}_{\text{adj}}$ to exceed the ‘normal’ VAL for all such geometries).

Under this approach for mitigating ionospheric anomalies, significant sigma inflation is required, which means that the current Category I architecture cannot be extended to support high availability of Category II or III landings without some improvements. One improvement would be the inclusion of airborne (as well as ground system) monitoring of ionospheric gradients. Another possible improvement is a more realistic, less-conservative ionospheric anomaly threat model that based partially on theoretical ionospheric behaviour models, in addition to extrapolation from recorded data. These improvements, combined with re-stated GBAS Category II/III requirements based on GBAS Service Level (GSL) D as defined in the most recent LAAS MASPS update, should make it possible to extend the current single-frequency GBAS architecture to support adequately the Category II/III operations. If not, dual-frequency GBAS would likely be needed to make high availability Category II/III operations possible.

Acknowledgements
The authors would like to thank Jason Rife, Jiyun Lee, Ming Luo, Godwin Zhang, Seebany Datta-Barua and Todd Walter of Stanford University, Boris Pervan and Livio Gratton of the Illinois Institute of Technology, Tom Dehel of the FAA William J Hughes Technical Center, and Mats Brenner of Honeywell for their help in studying the impact of ionospheric anomalies on GBAS. The advice and interest of many other people in the Stanford GPS research group is appreciated, as is funding support from the FAA LAAS Program Office. The opinions discussed here are those of the authors and do not necessarily represent those of the FAA or other government agencies.

References
28 Braff R & Shively C, Derivation of Ranging Source Integrity Requirements for the Local Area Augmentation System (LAAS), Navigation (France), 47, No. 4, (2000-2001), 279.