A Simple Method of Signal Quality Monitoring for WAAS LNAV/VNAV

Peter Shloss, *Raytheon Company*
R. Eric Phelts, Todd Walter, Per Enge, *Stanford University*

Biographies

Mr. Peter Shloss is a Senior Principal Systems Engineer with Raytheon Company and is technical director for the MSAS program. He has Bachelors and Masters degrees in Electrical Engineering from the University of Cincinnati and the University of Southern California, respectively, and has over 20 years of experience in systems engineering for commercial and military applications.

R. Eric Phelts is a Research Associate in the Department of Aeronautics and Astronautics at Stanford University. He received his B.S. in Mechanical Engineering from Georgia Institute of Technology in 1995, and his M.S. and Ph.D. in Mechanical Engineering from Stanford University in 1997 and 2001, respectively. His research involves multipath mitigation techniques and satellite signal anomalies.

Dr. Todd Walter received his B. S. in physics from Rensselaer Polytechnic Institute and his Ph.D. in 1993 from Stanford University. He is currently a Senior Research Engineer at Stanford University where his research focuses on algorithms that provide provable integrity for WAAS.

Per Enge is an Associate Professor of Aeronautics and Astronautics at Stanford University, where he has been on the faculty since 1992. His research deals with differential operation of GPS for landing aircraft. Previously, he was an Associate Professor of Electrical Engineering at Worchester Polytechnic Institute.

Abstract

The integrity of the Wide Area Augmentation System (WAAS), being developed for the FAA, is of significant concern because of its intended use in commercial aviation navigation applications. The current WAAS plan calls for several upgrades with each upgrade providing improved service coverage and availability at increasingly lower precision approach decision heights. The first planned deployment, LNAV/VNAV, will provide an approach service with both lateral and vertical guidance.

One of the threats to the integrity of the WAAS-corrected user position solution is that of an anomalous GPS broadcast signal, also known as an “evil waveform”. Detection of such distortion is made difficult due to the fact that the ranging error caused by such distortion is dependent on the spread spectrum receiver discriminator type, correlator spacing, and bandwidth. This leads to some potentially complex solutions for detection, involving multiple correlator spacings, etc.

This paper discusses the threats, detection requirements, and detector design approach used to mitigate the failures of concern to the WAAS LNAV/VNAV system. The approach used takes advantage of another detector already required for another type of satellite failure (code-carrier coherence failure). The analysis includes application of a model for receiver-specific distortion effects. This is used to translate error limits and thresholds between the “user” domain and the “detector” domain. The paper walks through the analysis to select thresholds that meet the allocated integrity (detection) and continuity (false alarm) requirements.

Introduction

The Wide Area Augmentation System (WAAS) is a safety-critical, software-intensive system, augmenting the satellite-based Global Positioning System (GPS). The system provides airborne users with positions of adequate accuracy, availability, continuity, and integrity to support different phases of flight. Under the "Free Flight" concept of the National Airspace System (NAS) adopted by the

The contents of this material reflect the views of the authors. Neither the Federal Aviation Administration nor the Department of Transportation make any warranty or guarantee, or promise, expressed or implied, concerning the content or accuracy of the views expressed herein.

Federal Aviation Administration (FAA) at the turn of the century, the GPS/WAAS infrastructure is assuming a critical role in ensuring the safe and efficient flight operating capability of the NAS.

The far-reaching impact on flight operations has made WAAS a safety-critical system. A system hardware or software failure or undetected GPS or WAAS satellite ranging failure has the potential to impact a significant volume of airspace and aircraft in the course of navigation or landing.

The WAAS system has a top level safety requirement to protect users at every point in space and time with 10^{-7} or better probability of integrity failure. Schempp [1] provides a top level description of the approach used to prove the algorithms meet their integrity requirements.

Each of several integrity monitors in the WAAS ground system is assigned a specific set of threats, which they are designed to mitigate. The system level integrity requirement is allocated to each monitor and hardware component in a manner that guarantees that the probability a user experiences HMI at any point in time during a 150 second approach is less than 10^{-7}.

This paper describes the code-carrier coherence (CCC) Monitor, which is designed to mitigate two possible threats to the User Differential Range Error (UDRE) values that are broadcast by WAAS. The UDRE represents an overbound of residual error for a given satellite ranging source (GPS or WAAS) after WAAS clock corrections are applied. These must properly bound the error, even when WAAS ground system hardware has failed or the GPS or WAAS satellite malfunctions.

The two threats mitigated by the integrity monitor described in this paper are satellite malfunctions. The specific malfunctions are: 1) a divergence between the satellite pseudorandom noise code and its radio frequency carrier, hereafter termed a code-carrier coherence (CCC) failure, and 2) a signal distortion of the pseudorandom code. This class of signal distortion failure was first observed on GPS satellite number 19, and is hereafter termed an SV-19 failure. The threats are described in detail later in the paper. The SV-19 threat is particularly troublesome, because the range error caused by this type of failure is dependent on the type of receiver used. This must be accounted for when establishing error limits and thresholds.

CCC Monitor Description

A satellite failure causing code-carrier divergence causes errors in the user's carrier smoothing of pseudorange measurements. The CCC monitor is designed to directly sense the user's error by computing the weighted average of multipath deviations (ionosphere-corrected code-carrier differences) for all receivers viewing the satellite. In the absence of code-carrier incoherence, the average should be near zero (assuming independent, random multipath at each receiver). In the presence of a ramping code-carrier divergence, the average will appear as a bias representing the error in pseudorange domain.

In contrast, a satellite failure causing signal deformation causes a pseudorange error (i.e., a step change in pseudorange) in the user that may be different from the error caused in the WAAS reference receiver. This is because of the allowable range of user receiver parameters (specifically, correlator spacing, discriminator type and bandwidth). This potential disparity makes the detector design problem more difficult for the signal deformation failure than for the code-carrier divergence failure. The generic term for the process of detecting signal deformation is signal quality monitoring (SQM).

The CCC Monitor is able to detect both code-carrier coherence and signal deformation failures at low enough levels to protect users given the uncertainty (e.g., UDRE and GIVE) levels that are being broadcast by WAAS to cover other unlikely events.

The CCC Monitor is based on the following basic equation, which forms the weighted average of the multipath deviations of all reference receivers tracking each satellite:

$$ccc^i = \frac{\sum_j \left[\mu_j^i \Big/ \left(\sigma_j^i\right)^2 \right]}{\sum_j \left[1 \Big/ \left(\sigma_j^i\right)^2 \right]}$$

where μ_j^i is the multipath deviation for reference receiver j and SV i , and σ_j^i is the multipath error standard deviation for reference receiver j and SV i. [3]

A satellite failure is declared when the code-carrier coherence test statistic, ccc^i, exceeds a threshold. The threshold is a variable dependant on the current UDRE to be broadcast for the satellite.

Threat Models

The CCC/SV-19 threats may be characterized as either a "step" (instantaneous change) or a linear "ramp" (gradual) divergence of the nominal incoming code and carrier signals. Since dual-frequency processing removes the expected divergence induced by the ionosphere, such additional detected changes are considered anomalous. The CCC threat is modeled as a constant rate of code-carrier divergence, identically affecting both the L1 and L2 signals. The SV19 threat (i.e., one caused by a satellite failure similar to that experienced by SV19 in 1993) is modeled as a step in the broadcast code phase while the carrier phase remains unaffected.

The CCC Threat Model

The CCC threat is modeled as a linear ramp affecting code and/or carrier. The L1-L2 bias is computed in the WAAS CP; different effects on the L1 and L2 signals would induce an error identical to an erroneous τ_{gd} value from a satellite. While the CCC monitor would also likely detect such a threat, WAAS has another monitor specifically designed to catch such a threat. Therefore the CCC monitor is analyzed against linear ramp divergences affecting the L1 and L2 signals identically. The magnitude of the ramp can take on any value.

The SV19 Threat Model- Full ICAO Model

Subtle failures of the signal generating hardware onboard the satellite may distort the incoming signal and result in erroneous pseudorange measurements. More specifically, these anomalous waveforms distort the correlation function generated within a GPS receiver. This affects code-tracking loops and leads to erroneous pseudorange measurements. Further, for receivers of different configurations (i.e., discriminator type, correlator spacings, and front end bandwidth) these correlation peak distortions result in different pseudorange errors. Since user receivers vary and differ from the reference receivers, these errors cannot, in general, be differentially corrected. For integrity, WAAS reference stations must monitor the satellite signals for these waveforms (i.e., employ SQM).

These anomalies model a combination of both digital and analog failure modes on the satellite signal-generating hardware. The digital parameter, Δ, models a lead or lag of the falling edge of the C/A code chip transition. The parameters f_d and σ model the frequency and damping of a (2nd-order) failed, analog filter response. The 2nd-order response is given by:

$$e(t) = \begin{cases} 0 & t \le 0 \\ 1 - \exp(-\sigma t)\left[\cos \omega_d t + \dfrac{\sigma}{\omega_d} \sin \omega_d t\right] & t \ge 0 \end{cases}$$

$$\omega_d = 2\pi f_d$$

Figure 1 illustrates an example of these waveforms for $f_d = 3$MHz, σ = 0.8MNepers/sec, Δ = 0.3.

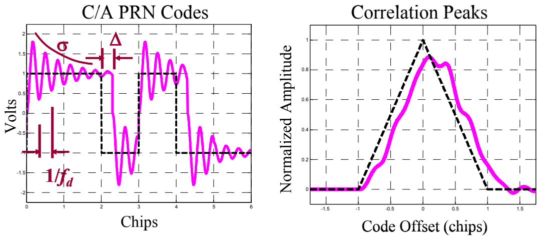

Figure 1. "2nd-Order Step" anomalous waveform with lead and the corresponding correlation peak

The SV-19 Most Likely Subset (MLS) Threat Model

The full ICAO model includes three subdivisions called threat models A, B and C. The initial build of WAAS protects against the "most likely subset," or MLS, of the full-ICAO threat model. The MLS includes only those waveforms most similar to those generated on SV19 in 1993. These waveform parameters result from examination of data taken from the 40m dish antenna at the Camp Parks Air Force base. The data includes oscilloscope traces of the distorted SV-19 C/A code in October of 1993.

Table 1: Summary of Threat Models and Parameters

	Full ICAO Model	Most Likely Subset Model
Threat Model A: Lead/Lag Only	$-0.12 \le \Delta \le 0.12$	$-0.04 \le \Delta \le 0.04$
Threat Model B: Amplitude Modulation Only	$\Delta = 0$ $4 \le f_d \le 17$ $0.8 \le \sigma \le 8.8$	None
Threat Model C: Lead/Lag Plus Amplitude Modulation	$-0.12 \le \Delta \le 0.12$ $7.3 \le f_d \le 13$ $0.8 \le \sigma \le 8.8$	$-0.04 \le \Delta \le 0.04$ $f_d = 10.23$ $1.8 \le \sigma \le 7.8$

In contrast to the full ICAO model, the MLS model only includes threat models A and C, and the parameter range for these two subsets is smaller than for the full ICAO model. Table 1 summarizes the relationships between these three parts.

The contents of this material reflect the views of the authors. Neither the Federal Aviation Administration nor the Department of Transportation make any warranty or guarantee, or promise, expressed or implied, concerning the content or accuracy of the views expressed herein.

Phase I WAAS mitigates the MLS waveforms. The MLS threat model conservatively models the SV-19 failure, which has occurred only once over the entire lifetime (over 20 years) of continuous GPS operation. The failure occurred on a Block II satellite; currently only four Block II satellites (or satellites with the same design and/or design components) are in operation and they are near end of life.

WAAS will employ offline monitoring equipped with special SQM receivers to constantly monitor the constellation for signal distortion of all types, and remove a satellite from the WAAS solution should the need arise. It is planned that these SQM receivers will be built into the WAAS system to lessen the system's dependency on offline monitoring. Under this design, WAAS will be able to autonomously protect against the full ICAO threat space.

Rising vs. Risen Case

For WAAS, CCC/SV19 failures fall into two distinct categories: the "Rising SV" case and the "Risen SV" case. The "Rising SV" case describes the instance where a GPS satellite experiences a CCC/SV19 failure before it is in view of the WRSs. In this case, the carrier measurements are leveled to the code as normal; however a bias due to the anomalous code distortion remains present and is undetectable by the CCC monitor. As illustrated in Figure 2, the bias becomes incorporated into the WAAS correction and is indistinguishable from a satellite clock offset. It is broadcast to the user as a part of the differential correction. As a result, some of the error, which will appear common-mode between the reference stations and the user, will cancel out. This (partial) cancellation acts to reduce the maximum pseudorange error any user can experience due to these waveforms.

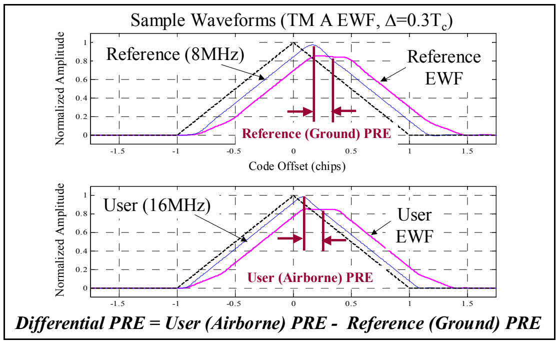

Figure 2. User Differential Pseudorange Errors (PREs) from Rising Satellites are Reduced by WRS (Reference) Corrections

The "Risen SV" case accounts for the instance where the satellite fails while it is in full view of the WAAS network. In this case, the code distortion does not immediately affect the broadcast correction because the carrier smoothing has reached steady state and that smoothing filter has a two-hour time constant. The WAAS correction will primarily propagate from SV-19-bias-free, carrier-leveled measurements. However, the failure will affect the user position solution, since the user employs a much shorter, 100-second time constant for carrier smoothing. Accordingly, as illustrated in Figure 3, larger user errors result from the Risen SV case. This case requires the CCC monitor to detect the failures.

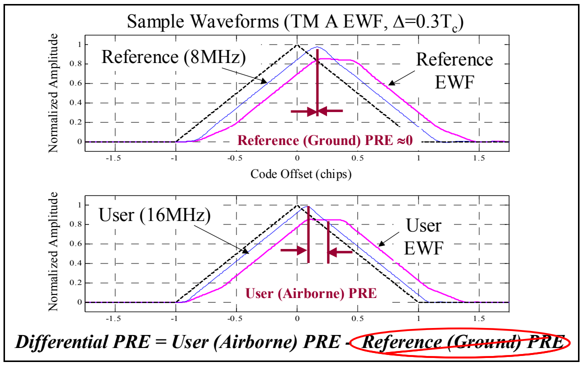

Figure 3. User Differential Pseudorange Errors (PREs) from Risen Satellites with SV19 Failures are Not Compensated by Corresponding Errors in Differential Corrections

Failure Rates

The *a priori* failure rate, $P_{f\_apriori}$, used for GPS CCC and SV-19 satellite failures is 1e-4 per hour. This number conservatively reflects the specified failure rate from the SPS Signal Specification [3] and appears to be very conservative. The analysis could leverage the fact that the failure — asserted to be a single, instantaneous transition from good to anomalous — occurred only once in the history of observations. By conservatively modeling it to occur once over the specified 10-year lifetime of a Block II satellite per satellite, the probability would become 1.14e-5 per hour. Using the longer constellation history and fact that it was observed on only one satellite could reduce that value by another order of magnitude. Therefore, the assumed rate is very conservative compared to the history of observation.

The WAAS ground system controls the GEOs' code-carrier coherence. WAAS has more failure modes that can contribute to such a problem than does a GPS satellite, and some deviations in code-carrier coherence have occurred in the past (although not large enough to exceed the allowable error level). Accordingly, the analysis uses an event probability

The contents of this material reflect the views of the authors. Neither the Federal Aviation Administration nor the Department of Transportation make any warranty or guarantee, or promise, expressed or implied, concerning the content or accuracy of the views expressed herein.

for GEO satellites of 1.14e-4 per hour, which is slightly higher than for GPS. This is based on no more than one observed event per year per GEO.

Monitor vs User Domain Errors

In this paper, the terms "detector" or "monitor domain" refer to issues relating to the monitoring and detecting of satellite failures. The term "user domain" refers to issues that produce errors in avionics receivers. "Margin" (either domain) refers to the difference between the maximum error tolerable for integrity. Detection thresholds are set in the monitor domain and, in part, determine these margins. Figure 4 graphically illustrates the relationship between errors in each domain.

In the monitor domain, there are two constraining factors on selection of the detection threshold. First, the threshold must be large enough that the false alarm rate does not cause excessive impact to system continuity. Second the threshold must be tight enough to meet the required missed detection probability, leading to the required P_{HMI} performance. The minimum detectable error (MDE) is defined as the minimum threshold value that meets both the continuity (false alarm) and missed detection requirements.

Margin in the monitor domain is defined as the amount that the threshold has been set below the maximum value permitted for integrity (while still providing the required false alarm/continuity). This can be computed in the monitor domain simply as the monitor error limit (L_{mon}) minus the MDE, where L_{mon} is computed by translating the user domain error limit to the monitor domain using the user domain to monitor domain curve.

Once the MDE is computed, it can also be translated back to the user domain using the monitor domain to user domain curve. The translation curve x and y axes are labeled PRE_{mon} and PRE'_{air}, respectively. PRE_{mon} is simply the pseudorange error in the monitor domain. PRE'_{air} is the maximum user differential range error over possible user receiver bandwidths and correlator spacings. (The general term for user pseudorange error PRE_{air}). PRE'_{air} maximizes PRE_{air} over discriminator type and PRE'_{air}(MDE) corresponds to the MDE as measured by the monitor. The margin in the user domain is simply the maximum allowable user range error (MERR) minus PRE'_{air}(MDE).

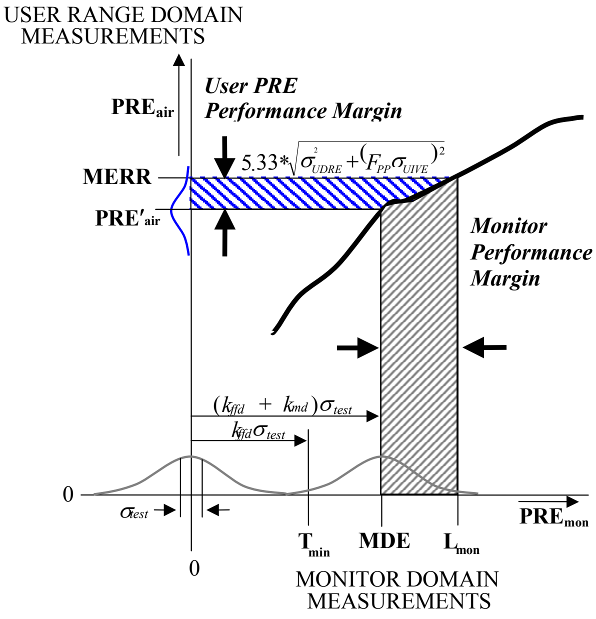
USER RANGE DOMAIN MEASUREMENTS
PRE_{air}
User PRE Performance Margin
$5.33*\sqrt{\sigma^2_{UDRE}+(F_{PP}\sigma_{UIVE})^2}$
MERR
PRE'_{air}
Monitor Performance Margin
$(k_{ffd} + k_{md})\sigma_{test}$
$k_{ffd}\sigma_{test}$
0
σ_{test}
PRE_{mon}
T_{min}
MDE
L_{mon}
0
MONITOR DOMAIN MEASUREMENTS

Figure 4. Monitor and User Domain Threshold and Margin Relationships

The CCC Monitor thresholds must be set (low enough) to provide the required missed detection probability for the worst case of the CCC and the SV-19 threats. (Note that for low values of UDREI, the SV-19 threat sets this threshold.) A CCC/SV-19 failure is declared if the code-minus-carrier residual exceeds a threshold, $T_{min} = T_{CCC} = (k_{ffd})\,\sigma_{test}$, where k_{ffd} is a fault-free detection multiplier associated with a zero-mean Gaussian probability distribution determined by the required false alarm probability, P_{fa}.

σ_{test} is the standard deviation of the CCC test statistic under fault-free conditions. Note that the same standard deviation is used for faulted conditions, since the fault under study simply introduces a bias in the test statistic.

The CCC monitor analysis, however, measures monitor performance by its ability to detect code-carrier incoherence at error values that meets both the false alarm and missed detection probability requirements. This is called the minimum detectable error (MDE). Accordingly, the MDE is given by

$$\mathrm{MDE} = (k_{ffd}+k_{md})\,\sigma_{test} = \mathrm{T}_{\mathrm{CCC}} + k_{md}\,\sigma_{test}$$

The contents of this material reflect the views of the authors. Neither the Federal Aviation Administration nor the Department of Transportation make any warranty or guarantee, or promise, expressed or implied, concerning the content or accuracy of the views expressed herein.

where k_{md} is the constant multiplier found from the required missed-detection probability, P_{md}, with the measurement error distribution in the faulted condition.

Threshold Analysis Overview

The process for determining the thresholds for the CCC Monitor is summarized in Figure 5.

For the SV-19 threat, the satellite failure parameters are used to set the parameter space for models of the user receiver (air) equipment and the ground reference/monitor (mon) equipment. This generates a "PRE'_{air} vs. PRE_{mon}" relation between monitor (detected) pseudorange error and actual user error. The PRE'_{air} (as opposed to PRE_{air}) indicates that this is a worst case user error over all allowable receiver configurations.

The maximum error range residual (MERR) for the user is computed based on the broadcast UDRE and GIVE floors in the system. These are translated to monitor error limits (L_{mon}) using the relation PRE'_{air} vs. PRE_{mon} derived above.

The required missed detection probability is computed based on the a-priori satellite failure rate and the overall P_{HMI} allocation for the SV-19 and CCC threats.

The continuity requirement is used to set a false alarm probability. Test statistics are characterized and used to compute minimum and maximum thresholds based on the P_{md} and P_{fa} computations. The final threshold selection is ideally a tradeoff between false alarm rate and missed detection margin. The final margin is computed first in the monitor domain and is then translated back to the user domain using the PRE'_{air} vs. PRE_{mon} relationship derived earlier.

A similar process is used to determine threshold requirements for the CCC threat. However, for CCC there is no need to perform the monitor-to-user translation, since the CCC monitor is directly sensing the code-carrier divergence. The only receiver-dependent parameter affecting this threat is the receiver carrier smoothing filter constant. The WRS receiver smoothing filter uses a shorter time constant (25 seconds) than the user (100 seconds), which actually makes the CCC monitor more sensitive to this threat than the user.

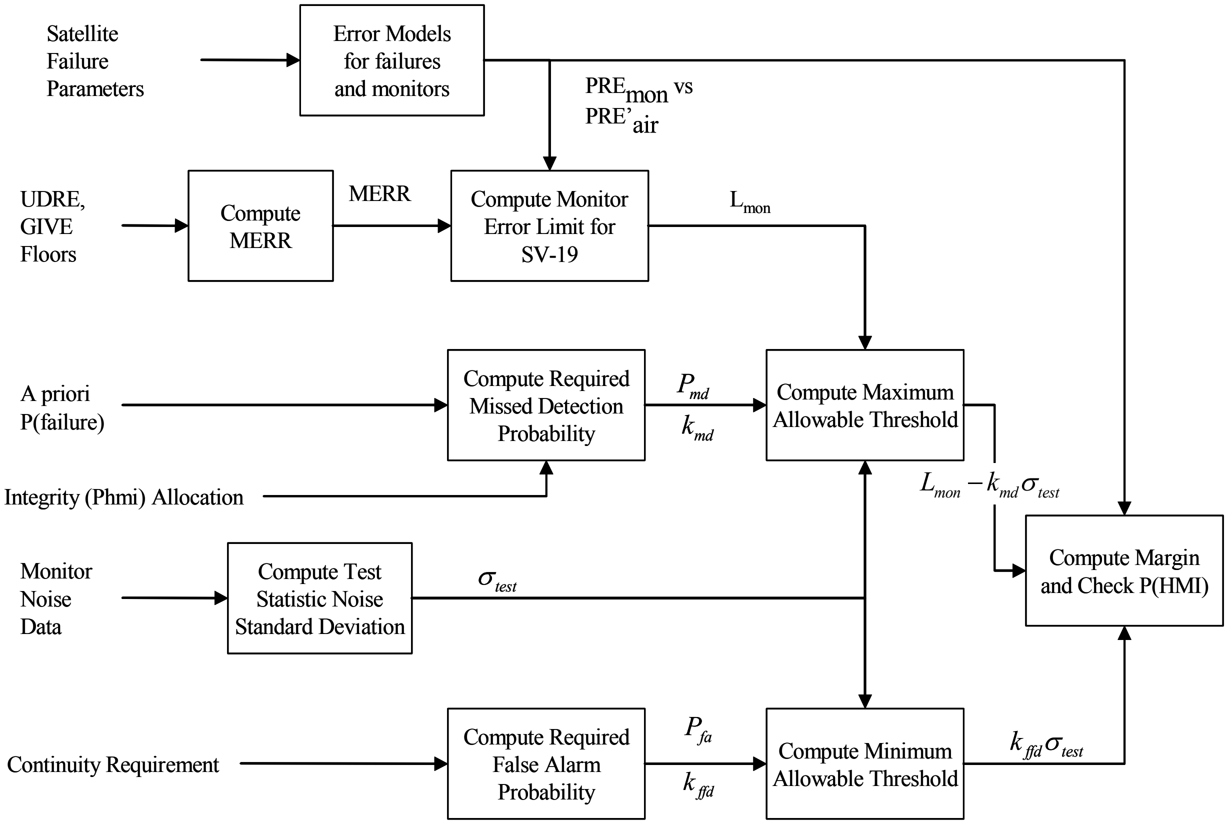
Satellite Failure Parameters
Error Models for failures and monitors
PRE$_{mon}$ vs PRE'$_{air}$
UDRE, GIVE Floors
Compute MERR
MERR
Compute Monitor Error Limit for SV-19
L_{mon}
A priori P(failure)
Compute Required Missed Detection Probability
P_{md}
k_{md}
Compute Maximum Allowable Threshold
Integrity (Phmi) Allocation
$L_{mon} - k_{md}\sigma_{test}$
Compute Margin and Check P(HMI)
Monitor Noise Data
Compute Test Statistic Noise Standard Deviation
σ_{test}
Continuity Requirement
Compute Required False Alarm Probability
P_{fa}
k_{ffd}
Compute Minimum Allowable Threshold
$k_{ffd}\sigma_{test}$

Figure 5. Threshold Analysis Overview

Error Limit Determination

MERR Derivation

The Maximum Error Range Residual (MERR) is the maximum allowable user domain pseudorange error, which depends upon σ_{UDRE} and σ_{GIVE_FLOOR}. It is a "minimum satellite protection level," which bounds the tolerable error on a (single) critical satellite. Any range error, on that critical satellite, at or above the MERR may cause a user to experience HMI.

The MERR is defined according to

$$MERR = 5.33 * \sqrt{\sigma_{UDRE}^2 + \left(F_{PP}\sigma_{UIVE}\right)^2}$$

where F_{PP} is the obliquity factor is conservatively set equal to unity for the MERR computation. σ_{UDRE} and σ_{UIVE} are the standard deviations of the UDRE and GIVE monitors. Under nominal conditions (e.g., no ground system hardware or software failures), both represent well overbounded quantities. For the MERR, σ_{UIVE} is conservatively set equal to the GIVE (Grid Ionospheric Vertical Error) floor value of 3.0 meters. (More about the WAAS GIVE monitor and its accompanying assertions and algorithms can be found in [4].)

Figure 6 shows the monitor versus user domain errors resulting from MLS waveforms for the Risen SV case. Each point plotted corresponds to the maximum user pseudorange error (PRE_{air}) resulting from a different waveform within the threat model. The horizontal axis, however, plots a conservative estimate of the WAAS reference receiver PREs. Note that for some waveforms, the CCC monitor—as measured by the WAAS reference receivers—observes no error, while a non-zero error will always exist for users of a given bandwidth, correlator spacing and discriminator type. Fortunately, this undetected level is below the minimum MERR.of 6.1 meters. The uppermost points correspond to the waveforms that create the maximum user errors for a specific CCC measurement, PRE_{gnd} (or PRE_{mon}). Further, these points correspond to PRE'_{air}, since they allow a direct comparison of any possible CCC MDE with its resulting maximum PRE_{air}. Note that the maximum user PRE (overall) is 8.32 meters and it occurs for users with ΔΔ receivers having a 14MHz bandwidth and a (narrowest) correlator spacing of 0.045 chips.

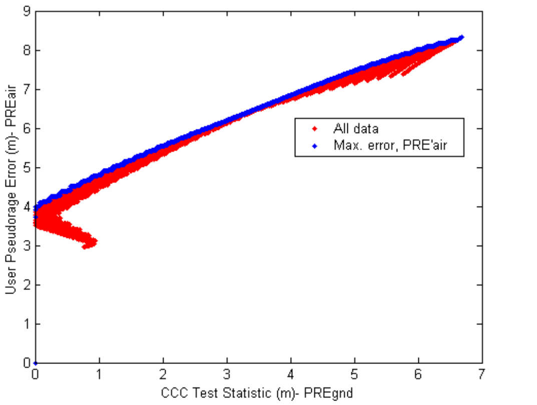

Figure 6. User Pseudorange Error vs. CCC Monitor Detected Error for the SV-19 (Risen Case Threat: TM_{MLS} C*, ΔΔ)

Using the data from Figure 6, the monitor error limit for SV-19 failures, L_{mon}, can be computed for each value of MERR (user domain error limit). Table 2 lists a partial table of values of MERR and L_{mon} as a function of UDRE Index (UDREI). Note that for CCC failures, the MERR applies directly.

Table 2. Maximum Error Range Residual (MERR) vs. UDRE Index (at the User)

UDREI	UDRE	MERR	L_{mon}
4	2.25	6.1	2.82
5	3	6.9	4.05
6	3.75	7.8	5.57

The same type of analysis that was performed to generate the plot of Figure 6 for the risen case was also performed for the rising case. For this case, due to cancellation of errors effect described earlier, the maximum user error is only 4.2 meters. Since this is less than the minimum MERR of 6.1 meters, no CCC monitor mitigation is needed.

SV-19 Threat Mitigation Strategy

Figure 7 summarizes the mitigation strategy for SV-19 threats for Phase 1 WAAS. It shows that the CCC Monitor is used to detect failures for the MLS portion of the ICAO threat model, and that mitigation is not required for the rising SV case. WAAS requires offline monitoring (using SQM receivers) to detect the correlation peak distortion and limit the exposure time to this pseudorange bias.

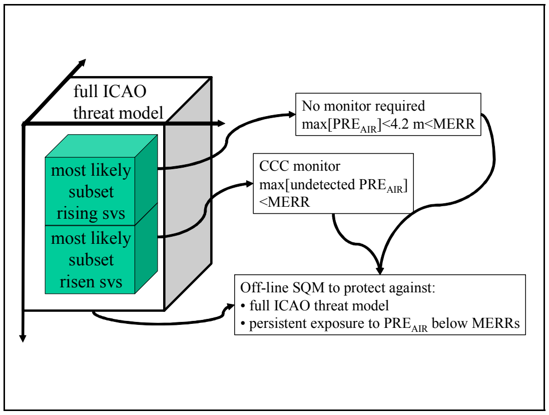
full ICAO
threat model
most likely
subset
rising svs
most likely
subset
risen svs
No monitor required
max[PRE$_{AIR}$]<4.2 m<MERR
CCC monitor
max[undetected PRE$_{AIR}$]
<MERR
Off-line SQM to protect against:
• full ICAO threat model
• persistent exposure to PRE$_{AIR}$ below MERRs

Figure 7: Summary of Phase I WAAS Strategy for SQM

Test Statistic Characterization

Since the missed detection probability is a function of the monitor noise standard deviation, σ_{test}, and the detection threshold, proper characterization is critical. For this analysis, σ_{test} resulted from a zero-mean Gaussian overbound of histograms of ccc^j formed from eight days of recorded live receiver measurement data. Since the algorithm computes statistics every second for each satellite in view of WAAS, the histograms were well populated. Separate histograms were collected for each indexed value of UDRE, for L1 and L2, and for GPS versus GEO SVs, since the test thresholds are also per UDRE index. At the minimum UDRE value used for this phase of WAAS, σ_{test} for GPS SVs (corresponding to the tightest test threshold), was found to be 0.23 meters.

Test Threshold and Margin Computation

As an example, the threshold and margin analysis is described for the SV-19 GPS failure case. The CCC monitor targets a maximum false alarm rate of one per satellite per year. This value was chosen to make the impact to user service continuity negligible. If the exposures to false alarms are independent from second-to-second, this results in a P_{fa} of 3.2×10^{-8} false alarms per satellite per second (for all approach cases). This corresponds to a k_{ffd} of 5.54.

P_{md} is found from the fault tree P_{HMI} allocations and a priori satellite failure rate probabilities, $P_{f\_apriori}$. The integrity risk (P_{HMI} allocations) for this monitor from the P_{HMI} fault tree and the GPS SV-19 threats is 8.333e-10/ approach. For $P_{f\_apriori}$ =1e-4, the P_{md} requirement for GPS SV-19 failures is 8.33e-6. This corresponds to a k_{md} of 4.46.

Given a value of σ_{test} , the missed detection and false alarm probability requirements, and the error limits, computing thresholds is straightforward. Table 3 summarizes the results for the GPS SV-19 case.

Table 3. Threshold Analysis Results (GPS SV-19, PA) (all units are meters)

UDREI	σ_{test}	T_{min}	MDE in Monitor Domain	MDE in User Domain	Monitor Domain Margin	User Domain Margin
4	0.23	1.27	2.30	5.8	0.52	0.28
5	0.35	1.94	3.50	6.5	0.55	0.37
6	0.36	1.99	3.60	6.6	1.97	1.18

Special Considerations

PHMI Computation

The preceding analysis was performed assuming other errors in the system were negligible. In order to verify that the resulting margin is sufficient, there is an additional confirmation step. This computes the P_{HMI} accounting for nominal correction errors (satellite clock and ephemeris, ionosphere) present in the system. Accordingly, it is found from

$$P_{HMI} = 1 - \Phi\left(\frac{MERR - PRE'_{air}\left(MDE\right)}{\sqrt{\sigma^2_{UDRE\_nom} + \sigma^2_{GIVE\_nom}}} \right)$$

where PRE'air(MDE) is the maximum expected user PRE that may exist on the satellite due to an *undetectable* CCC/SV19 signal fault. $\Phi(x)$ represents the cumulative distribution function for a zero-mean Gaussian evaluated at x. The amount of margin, MERR-PRE'$_{air}$, directly determines the value of PHMI; the smallest margin (determined analytically) dictates the final PHMI for the CCC monitor.

Satellite "Lock-out"

The CCC Monitor is based on multipath deviations computed by the CNMP monitor [2]. The CNMP monitor solves for carrier phase ambiguity using a filter with 2-hour time constant. This will, over time, act to reduce any change in pseudorange (relative to a leveled carrier) that would be observed by the CCC Monitor for an SV-19 failure. Accordingly, a satellite that fails the CCC monitor test will be removed from the WAAS solution (by setting it to "Do Not Use.") long enough to finish the current satellite pass (9 hours). Provided Offline Monitoring does not intervene, it may re-enter the WAAS solution provided it passes a CCC check.

The contents of this material reflect the views of the authors. Neither the Federal Aviation Administration nor the Department of Transportation make any warranty or guarantee, or promise, expressed or implied, concerning the content or accuracy of the views expressed herein.

User Carrier Smoothing Filter Reset

WAAS integrity requirements dictate not only that HMI is prevented with high probability, but also that an HMI condition, if present is corrected within a short time-to-alarm. In the case of the CCC Monitor, a particular scenario was identified that placed potential stress on meeting the time-to-alarm requirement. The scenario occurs when the user's carrier smoothing filter reset at the same time as a (ramp) CCC failure occurs. Under these conditions, the user may experience temporary large errors as the smoothing filter is warming-up. At the same time, the reference receivers that are supplying data to the CCC Monitor may not have reset their smoothing filters, and would therefore be sensing (temporarily) less error. This scenario was modeled for varying ramp divergence rates to show that the time-to-alarm requirement could be met.

Offline Monitoring

The CCC monitor relies on Offline Monitoring to detect, identify, and remove SV-19-like signal distortions, which may not cause HMI, but may still pass undetected by the monitor. Offline Monitoring will act to keep any similar fault-induced ranging biases from continuing to corrupt user range measurements.

The FAA Technical Center will employ six multi-correlator SQM receivers to monitor for signal distortion from both the MLS and full ICAO threat models. These receivers will be distributed across CONUS to detect and identify these types of signal anomalies should they occur anywhere WAAS is available to users.

Conclusions

This paper presents a simple method for performing signal quality monitoring. WAAS will use its CCC monitor to detect the code-carrier divergence this class of failures—anomalous code signal distortion—introduces. The CCC monitor easily detects these faults if the satellite has already risen and is in view of the WAAS network. It cannot mitigate this threat if the signal distortion occurs before the satellite rises into view. However, the maximum user errors for this latter case will not result in HMI for the user.

Note that this method is valid only for the types of failures most similar to the original SV19 failure encapsulated by the most likely subset (MLS) of the full-ICAO threat model. Subsequent phases of WAAS will employ true, multi-correlator SQM receivers to detect the hazardous ICAO waveforms in real-time [5]. For Phase I WAAS, however, offline monitoring is used to perform this task.

Acknowledgements

The authors would like to acknowledge that this effort was sponsored by the FAA Satellite Program Office. The authors would also like to acknowledge participants of the WAAS Integrity Performance Panel for their constructive comments on the CCC Monitor design and analysis. In particular, Karl Shallberg deserves recognition for early work on the monitor sensitivity. In addition, thanks to A.J. Van Dierendonck for pointing out the rising versus risen case issue.

References

[1] T. Schempp, S. Peck, R. Fries, "WAAS Algorithm Contribution to Hazardously Misleading Information (HMI)", ION GPS 2001, September 2001.

[2] K. Shallberg, P. Shloss, E. Altshuler, L. Tahmazyan, "WAAS Measurement Processing, Reducing the Effects of Multipath", ION GPS 2001, September 2001.

[3] Global Positioning System Standard Positioning Service Signal Specification, Department of Defense, June 2, 1995.

[4] T. Walter, et al, "Robust Detection of Ionospheric Irregularities," ION GPS 2000, September 2000.

[5] R. Phelts, D. Akos, P. Enge, "Robust Signal Quality Monitoring and Detection of Evil Waveforms," ION GPS 2000, September 2000.

The contents of this material reflect the views of the authors. Neither the Federal Aviation Administration nor the Department of Transportation make any warranty or guarantee, or promise, expressed or implied, concerning the content or accuracy of the views expressed herein.