Advanced RAIM User Algorithm Description: Integrity Support Message Processing, Fault Detection, Exclusion, and Protection Level Calculation

Juan Blanch, Todd Walter, Per Enge.
Stanford University

Young Lee
MITRE/CAASD

Boris Pervan
Illinois Institute of Technology

Markus Rippl, Alex Spletter
German Aerospace Center

ABSTRACT

Advanced RAIM (ARAIM) for vertical guidance has attracted considerable attention both from integrity providers and receiver manufacturers, due to its potential to achieve worldwide coverage of vertical guidance with a reduced investment on the ground segment compared to Satellite-based Augmentation Systems. Several user algorithms have been published, mostly variants of solution separation and possible optimizations. These descriptions have focused on the definition of the Vertical Protection Level (VPL), because that is what was needed to simulate ARAIM availability as a function of the input parameters and the constellation configurations. However, an ARAIM user algorithm has many more elements that need to be defined. The purpose of this work is to describe an Advanced RAIM user algorithm step-by-step including: the Integrity Support Message (ISM) processing, the fault detection and exclusion, and the Protection Level calculation – including the Horizontal Protection Level. In this description, we attempt to clarify areas that have remained undefined.

We propose the contents of the ISM, and a clarification of the interpretation of its parameters. These parameters describe both the nominal error behavior and the probability of fault on one or more satellites. The nominal error is characterized by two sets of standard deviation and maximum bias, the first one for integrity purposes and the second one, less conservative, for accuracy and continuity evaluation purposes. We show how to compute the nominal error model as a function of the ISM content, and how to determine which fault modes must be monitored – including which subset solutions must be computed and compared against the all-in-view solution.

In this paper, we make explicit under which conditions a fault must be declared. In addition to the solution separation statistics, we show why it is prudent to include an additional chi-square test on the residuals. We also describe the actions that follow the detection of a fault or faults, and under which conditions fault exclusion can be performed. Although this is not expected to be fundamentally different from the current approaches taken in horizontal RAIM, there are differences that arise.

As mentioned above, the Vertical Protection Level has been defined in several publications (each with small variations). In this paper we address the implementation details for both the VPL and the HPL. First, in case a large number of fault modes need to be monitored, a large number of subset solutions must be computed. We show how to efficiently compute the subset solutions. Second, the PLs that provide good availability typically require an iterative halving algorithm. We describe a method to compute a tight upper bound with very few steps. In addition, we provide the formulas for the Effective Monitor Threshold, the fault free 10^{-7} error bound, and the 95% bound on the accuracy. A concrete numerical example is given to facilitate the verification of the provided formulas and algorithms.

1. INTRODUCTION

GPS with Receiver Autonomous Integrity Monitoring (RAIM) has been used for aircraft navigation since the mid-nineties [1], [2]. Today, RAIM guarantees horizontal error bounds of one nautical mile worldwide with high availability, and down to 0.3 nautical miles with somewhat reduced availability, without additional ground infrastructure [3], [4], [5]. With the deployment of new GNSS constellations and new signals in Aeronautical Radio Navigation Service (ARNS) bands, there is a strong interest to expand the role of RAIM in aircraft navigation [6].

It is expected that at the end of this decade there will be at least three GNSS constellations with signals in the L1/E1 and L5/E5a frequency bands: GPS, Galileo, and COMPASS [7]. The increased number of satellites in view will improve the user geometry, and the new signals in L5/E5a will allow receivers to cancel the first order ionospheric delay which is the largest source of pseudorange error uncertainty. In addition, in the case of GPS, there have been significant gains in clock and ephemeris accuracy as well as satellite reliability in the last decade [32].

These improvements have naturally led to consider the use of RAIM for more demanding phases of flight, in particular those requiring vertical guidance. There are currently 2939 Localizer Performance with Vertical guidance (LPV) approach procedures [8] in the U.S (more than twice the number of ILS approaches) [40]. These procedures, which are almost equivalent to Category I precision approaches, have very stringent requirements on the navigation error. For LPV-250, which allows minima down to 250 feet, any vertical position error larger than 50 m (the Vertical Alert Limit (VAL)) must be flagged to the pilot within 6s (with a probability larger than $1\text{-}10^{-7}$). For LPV -200, which allows minima down to 200 feet, the VAL goes down to 35 m. Currently, these procedures are supported by Satellite Based Augmentation Systems (SBAS). An SBAS receiver assesses the availability of an LPV-200 approach by computing a Vertical Protection Level (VPL) and a Horizontal Protection Level (HPL) (which are 10^{-7} error bounds on the vertical and horizontal position errors respectively).

The GPS Evolutionary Architecture Study (GEAS) outlined an Advanced RAIM concept in the GEAS Phase II report [6], which has been further developed within the Working Group C ARAIM Technical subgroup (ARAIM SG) [9]. This ARAIM concept relies on a ground system to provide periodic updates regarding the nominal performance and fault rates of the multiplicity of contributing constellations. This integrity data is contained in the Integrity Support Message (ISM) that is determined on the ground and broadcast to the airborne fleet [9], [10].

Since the GEAS Phase II Report [6], it has become apparent that multiple simultaneous faults cannot be ruled out, and therefore might need to be mitigated by the airborne receiver. The user algorithm described in [6] only covered the single fault case. Although it was indicated that the algorithm could be generalized to multiple failures, the exact implementation was not made explicit. Methods to compute the Protection Levels with threat models including multiple faults have been described in [11], [12], [13]. The present work describes each step of an ARAIM user algorithm based on these references.

Section 2 describes some of the performance requirements that need to be met by the ARAIM user algorithm, and motivates the need for additional availability criteria. Section 3 describes the main elements of the reference user algorithm step by step for ARAIM, and is an extension of the one described in the GEAS Phase II Report [6], including elements of [11], [12], and [13]. The algorithm is described in the order it is executed, starting with the calculation of the nominal error models and ending with the exclusion function. Section 4 summarizes possible improvements of the reference algorithm investigated by the ARAIM SG.

2. NAVIGATION REQUIREMENTS

The target operational level for ARAIM is LPV-200, which is a relatively new operation and one that is incompletely specified in the ICAO Standards And Recommended Practices (SARPs) [14]. Currently, LPV-200 is only provided by SBAS. The SARPs contain both requirements and guidance material on the desired operational performance, including positioning performance, continuity, and availability. However, ARAIM will have different characteristics than current SBAS, and it is important to understand how these differences may affect operational behaviour and the feasibility of meeting LPV-200 requirements. SBAS is a differential system that has better accuracy than the one expected for ARAIM. Furthermore, there is a concern that the test statistics in ARAIM, while protecting against errors exceeding the VAL, could allow large errors to remain undetected (for vertical guidance, it is not sufficient to have position errors below the VAL). Therefore, it is necessary to understand the operational requirements of LPV-200 and ensure the final ARAIM algorithm addresses these concerns.

For continuity, the SARPs specify a continuity risk requirement of 8×10^{-6} per 15 s. For ARAIM, the airborne algorithm tests have a finite probability of false alert, which can cause a loss of continuity. For this reason, a fraction P_{fa} of the total continuity budget must be allocated to the airborne algorithm.

The SARPs describe four vertical positioning performance criteria:

- 4 m, 95% accuracy;
- 10 m, 99.99999% fault-free accuracy;
- 15 m, 99.999% Effective Monitoring Threshold (EMT); and
- 35 m, 99.99999% limit on the position error, (i.e., the VPL has to be below a VAL of 35m).

Two of the criteria: 95% accuracy and VPL are described in Chapter 3 of Annex 10, Volume 1, of the ICAO SARPs [14]. The other two criteria: fault-free accuracy and EMT, are only described in the guidance material in Attachment D to Annex 10 which also provides more information on the previous two criteria. For the Wide Area Augmentation System (WAAS), it was determined by the Federal Aviation Administration (FAA) that if the VPL requirement is met, the other conditions are also all met. This is because of the inherent accuracy of WAAS and that the VPL is driven by rare fault-modes. Any condition that supported a VPL below 35 m, also assured that the accuracy requirements and EMT would be met.

ARAIM will have different error characteristics than SBAS. Unlike any SBAS, ARAIM makes use of the dual-frequency ionosphere-free pseudorange combination. Additionally, ARAIM does not use differential corrections. Therefore, it will likely have worse accuracy than current SBAS systems. Further, its method of error detection may allow fault modes to create larger position errors before they are identified and removed. Thus, conditions that support an ARAIM VPL below 35 m may not always lead to error characteristics that support LPV-200 operations.

Therefore, we introduce two additional other real-time tests in the aircraft to ensure that every supported condition has error characteristics that meet the intent of the SARPs. Specifically an accuracy test and an EMT test are described in Section 3. A single accuracy test assures that both the 4 m 95% and the 10 m 99.99999% test are met (since the tests are of identical form, but the 10 m test is more stringent). The EMT test prevents faults that are not large enough to ensure detection from creating vertical position errors greater than 15 m more often than 0.00001% of the time.

As was described in [6] and [9], there are two error models: an integrity error model and an accuracy (or continuity) error model (Appendix A). The integrity error model is used in the terms that have an impact on the integrity requirements, whereas the accuracy error model is used for all the other ones. More details can be found in [6] and [9].

3. ARAIM USER ALGORITHM

Definitions

y: vector of pseudorange measurements minus the expected range for an all-in-view position solution

x: receiver position and clock states (offset with respect to a position close enough to the true position so that the linear approximation of the observation equation is valid)

G: geometry matrix in East North Up (ENU) coordinates with a clock component for each constellation

Q: tail probability of a zero mean unit normal distribution. The *Q* function is defined as:

$$Q(u) = \frac{1}{\sqrt{2\pi}} \int_u^{+\infty} e^{-\frac{t^2}{2}} dt \quad (1)$$

Q^{-1}:inverse of the *Q* function.

PL: Protection Level

List of inputs

Name	Description	Source
PR_i	Pseudorange for satellite *i* after dual frequency correction, tropospheric correction, and smoothing are performed	Receiver
$\sigma_{URA,i}$	standard deviation of the clock and ephemeris error of satellite *i* used for integrity	ISM
$\sigma_{URE,i}$	standard deviation of the clock and ephemeris error of satellite *i* used for accuracy and continuity	ISM
$b_{nom,i}$	maximum nominal bias for satellite *i* used for integrity	ISM
$P_{sat,i}$	prior probability of fault in satellite *i* per approach	ISM
$P_{const,j}$	prior probability of a fault affecting more than one satellite	ISM

	in constellation *j* per approach	
$I_{const,j}$	index of satellites belonging to constellation *j*	Receiver
N_{sat}	number of satellites	Receiver
N_{const}	number of constellations	Receiver

The reference version of the Integrity Support Message contains $\sigma_{URA,i}$, $\sigma_{URE,i}$, $b_{nom,i}$, and $P_{sat,i}$ for each satellite *i;* and $P_{const,j}$ for each constellation *j*.

List of constants

Name	Description	Value (preliminary)
PHMI	total integrity budget	10^{-7}
$PHMI_{VERT}$	integrity budget for the vertical component	9.8×10^{-8}
$PHMI_{HOR}$	integrity budget for the horizontal component	2×10^{-9}
P_{CONST_THRES}	threshold for the integrity risk coming from unmonitored constellation faults	4×10^{-8}
P_{SAT_THRES}	threshold for the integrity risk coming from unmonitored satellite faults	4×10^{-8}
P_{FA}	continuity budget allocated to disruptions due to false alert. The total continuity budget is 8×10^{-6} per approach [14].	4×10^{-6}
P_{FA_VERT}	continuity budget allocated to the vertical mode	3.9×10^{-6}
P_{FA_HOR}	continuity budget allocated to the horizontal mode	9×10^{-8}
P_{FA_CHI2}	continuity budget allocated to the chi-square test	10^{-8}
TOL_{PL}	tolerance for the computation of the Protection Level	5×10^{-2} m
K_{ACC}	number of standard deviations used for the accuracy formula	1.96
K_{FF}	number of standard deviations used for the 10^{-7} fault free vertical position error	5.33
P_{EMT}	probability used for the calculation of the Effective Monitor Threshold	10^{-5}
T_{CHECK}	Time constant between consistency checks of excluded satellites	300 s
T_{RECOV}	Minimum time period a previously excluded satellite remains out of the all-in-view position solution	600 s

Pseudorange covariance matrices C_{int} and C_{acc}

The first step of the reference ARAIM algorithm proposed consists in computing the pseudorange error diagonal covariance matrices C_{int} (the nominal error model used for integrity) and C_{acc} (the nominal error model used for accuracy and continuity). They are defined by:

$$C_{int}(i,i) = \sigma_{URA,i}^2 + \sigma_{tropo,i}^2 + \sigma_{user,i}^2$$

$$C_{acc}(i,i) = \sigma_{URE,i}^2 + \sigma_{tropo,i}^2 + \sigma_{user,i}^2 \quad (2)$$

Preliminary error models for $\sigma_{tropo,}$ and $\sigma_{user,i}$ for both Galileo and GPS are given in Appendix A.

Results of this step: C_{int} and C_{acc}

All-in-view position solution

To be included in the all-in-view position solution, a satellite must not have been flagged in the last T_{RECOV} period and have a valid set of input parameters from the ISM. The all-in-view position solution $\hat{x}^{(0)}$ is computed as defined in Appendix E of [15]. A weighted least-squares estimation is performed at each iteration. The update for $\Delta\hat{x}$ is given by:

$$\Delta\hat{x} = \left(G^T W G\right)^{-1} G^T W \Delta PR \quad (3)$$

The geometry matrix G is an N_{sat} by $3+N_{const}$ matrix, where N_{const} is the number of independent constellations. The first three columns of G are defined as in Appendix E of [15]. Each of the remaining columns corresponds to the clock reference of each constellation. Labeling the constellations from j=1 to N_{const}, we define:

$$G_{i,3+j} = 1 \text{ if satellite } i \text{ belongs to constellation } j$$
$$G_{i,3+j} = 0 \text{ otherwise} \quad (4)$$

The weighting matrix W is defined as:

$$W = C_{int}^{-1} \quad (5)$$

ΔPR is the vector of pseudorange measurements minus the expected ranging values based on the location of the satellites and the position solution given by the previous iteration. When the position solution has converged, the last ΔPR is the vector y as defined above.

Results of this step: y, G, $\hat{x}^{(0)}$

Determination of the faults that need to be monitored and the associated probabilities of fault

The ISM does not specify explicitly which fault modes need to be monitored, and the corresponding prior probabilities which need to be assigned. This determination must be made by the receiver based on the contents of the ISM, in particular $P_{sat,i}$ and $P_{const,j}$ (introduced above in the list of inputs). Appendix C describes an algorithm that forms the list of fault modes (indexed by k) and their probabilities $p_{fault,k}$ as a function of the ISM. The index $k=0$ corresponds to the fault free case. A summary of the approach is provided below.

Independent simultaneous satellite faults

First, we determine the maximum number $N_{sat,max}$ of simultaneous satellite faults that need to be monitored. To compute $N_{sat,max}$, we define the probability of of all subset faults of size r and more. This probability will be noted $P_{sat\_subsets}(r,P_{sat,1},\ldots,P_{sat,Nsat})$. The number $N_{sat,max}$ is defined by:

$$N_{sat,\max} = \min\left\{ r \in 1,\cdots,N_{sat} \mid P_{sat\_subsets}\left(r+1, P_{sat,1},\cdots,P_{sat,N_{sat}}\right) \le P_{SAT\_THRES} \right\} \quad (6)$$

Appendix C provides an explicit way of determining the above number and an upper bound of $P_{sat\_subsets}(r,P_{sat,1},\ldots,P_{sat,Nsat})$. We define:

$$P_{sat,not\ monitored} = P_{sat\_subsets}\left(N_{sat,\max}+1, P_{sat,1},\cdots,P_{sat,N_{sat}}\right) \quad (7)$$

Once $N_{sat,max}$ is determined, all subsets with N_{sat}-$N_{sat,max}$ or more satellites are formed. We note idx_k the indices of the satellites included in subset k (this subset is used to monitor the fault indexed by k). For subset idx_k = $[1,N_{sat}]\backslash\{i_1, \ldots, i_r\}$ the corresponding probability is given by:

$$p_{fault,k} = \prod_{s=1,\ldots,r} P_{sat,i_s} \quad (8)$$

To illustrate this step, assume there are 20 satellites (N_{sat} = 20), all with $P_{sat}= 10^{-4}$. We have:

$$P_{sat\_subsets,\ upper\ bound}\left(3, P_{sat,1},\ldots,P_{sat,N_{sat}}\right) = 1.33\times10^{-9} \text{ / approach} \quad (9)$$

$N_{sat,max}$, the maximum number of simultaneous satellite failures that needs to be considered, is therefore two, because the contribution of all subset faults with three or more satellites is only a fraction of the total integrity budget. There are 20 one-satellite subsets and 190 two-satellite subsets. The contribution from all three-or-more fault cases is below 1.33 10^{-9}.

Constellation faults

In a similar way, we determine the maximum number $N_{const,max}$ of simultaneous constellation faults that need to be monitored. Although it is very unlikely that $N_{const,max}$ would exceed one, Appendix C indicates here how to determine it for arbitrary values. As with satellite faults, we must have:

$$P_{const\_subsets}\left(N_{const,\max}+1, P_{const,1},\ldots,P_{const,N_{const}}\right) \le P_{CONST\_THRES} \quad (10)$$

We define:

$$P_{const\_subsets}\left(N_{const,\max}+1, P_{const,1},\ldots,P_{const,N_{const}}\right) \quad (11)$$

In the case of two constellations with a prior of 10^{-4}, the probability of two simultaneous constellation faults is 10^{-8}, which is below the threshold P_{CONST_THRES}. There are therefore two fault modes that need to be monitored, one corresponding to each constellation fault.

Combined satellite – constellation faults

The combination of constellation and satellite faults is not considered at this time, as we expect this probability to be negligible. However, we can generalize the approach above the modes derived from the combined constellation and satellite fault. The idea is the same as above, but without distinguishing satellites and constellation faults. We define $N_{sat-const,max}$ as:

$$N_{sat-const,\max} = \min \left\{ \begin{array}{l} r \in 1,\cdots,N_{sat}+N_{const} \mid \\ P_{sat\_const\_subsets}\left(r+1,P_{sat,1},\cdots,P_{sat,N_{sat}},P_{const,1},...,P_{const,N_{sonst}}\right) \\ \le P_{SAT\_THRES}+P_{CONST\_THRES} \end{array} \right\}$$

The number $N_{sat-const,max}$ is now the number of simultaneous faults that needs to be monitored (satellite or constellation faults).

Results of this step: $p_{fault,k}$,idx_k for k ranging from 1 to the maximum number of fault modes to be monitored ($N_{fault\ modes}$), $P_{sat,not\ monitored}$, and $P_{const,not\ monitored}$

Fault-tolerant positions and associated standard deviations and biases

The monitor chosen to protect against the list of threats determined in the previous section is solution separation. Appendix G shows that, under certain assumptions, it is the optimal statistic.

For each k from 1 to $N_{fault\ modes}$, the difference $\Delta\hat{x}^{(k)}$ between the fault-tolerant position $\hat{x}^{(k)}$ and the all-in-view position solution $\hat{x}^{(0)}$, the standard deviations, and test thresholds are determined. For each k, we compute the diagonal weighting matrix:

$$\begin{array}{l} W^{(k)}(i,i) = C_{int}^{-1}(i,i) \text{ if } i \text{ is in } idx_k \\ W^{(k)}(i,i) = 0 \text{ otherwise} \end{array} \quad (12)$$

For all j such that:

$$\left(G^T W^{(k)}\right)_{3+j,\cdot} = \left[\begin{array}{ccc} 0 & \cdots & 0 \end{array}\right]^T \quad (13)$$

G must be redefined by removing its $3+j^{th}$ column. This happens if all satellites from constellation j are in idx_k.

The position solution tolerant to fault mode k is obtained by applying the corresponding weighted least squares to the residuals y:

$$\begin{array}{l} \Delta\hat{x}^{(k)} = \hat{x}^{(k)} - \hat{x}^{(0)} = \left(S^{(k)} - S^{(0)}\right) y \text{ where} \\ S^{(k)} = \left(G^T W^{(k)} G\right)^{-1} G^T W^{(k)} \end{array} \quad (14)$$

The computation of $S^{(k)}$ should take advantage of the relationship between $S^{(0)}$ and $S^{(k)}$ through rank one updates (in the case of a multiple satellite fault mode, more than one rank update is necessary) . The rank one updates formulas are given in Appendix I.

Let the index q = 1, 2, and 3 designate the East, North and Up components respectively. The variances of $\hat{x}_q^{(k)}$ for q from 1 to 3 are given by:

$$\sigma_q^{(k)2} = \left(G^T W^{(k)} G\right)^{-1}_{q,q} \quad (15)$$

The worst case impact of the nominal biases $b_{nom,i}$ on the position solution $\hat{x}_q^{(k)}$ is given by:

$$b_q^{(k)} = \sum_{i=1}^{N_{sat}} \left|S_{q,i}^{(k)}\right| b_{nom,i} \quad (16)$$

We compute the variance of the difference, $\Delta\hat{x}_q^{(k)}$, between the all-in-view and the fault tolerant position solutions:

$$\sigma_{ss,q}^{(k)2} = e_q^T \left(S^{(k)} - S^{(0)}\right) C_{acc} \left(S^{(k)} - S^{(0)}\right)^T e_q \quad (17)$$

in which e_q denotes a vector whose q^{th} entry is one and all others are zero.

Results of this step: $\sigma_q^{(k)}$, $\sigma_{ss,q}^{(k)}$, $b_q^{(k)}$ for k from 0 to $N_{fault\ modes}$, and from q from 1, 2, and 3.

Solution separation threshold tests and chi-square test

Solution Separation Test

For each fault mode, there are three solution separation threshold tests, one for each coordinate. The thresholds are indexed by the fault index k and the coordinate index q and noted $T_{k,q}$. They are defined by:

$$T_{k,q} = K_{fa,q} \sigma_{ss,q}^{(k)} \quad (18)$$

where:

$$K_{fa,1} = K_{fa,2} = Q^{-1}\left(\frac{P_{FA\_HOR}}{4N_{fault\ modes}}\right) \quad (19)$$

$$K_{fa,3} = Q^{-1}\left(\frac{P_{FA\_VERT}}{2N_{fault\ modes}}\right) \quad (20)$$

$Q^{-1}(p)$ is the (1-p)-quantile of a zero-mean unit-variance Gaussian distribution. Protection Levels can be computed only if for all k and q we have:

$$\tau_{k,q} = \frac{\left|\hat{x}_q^{(k)} - \hat{x}_q^{(0)}\right|}{T_{k,q}} \leq 1 \quad (21)$$

If any of the tests fails, exclusion must be attempted.

χ^2 statistic and threshold

The chi-square statistic for the all-in-view set is computed as follows:

$$\chi^2 = y^T\left(W_{acc} - W_{acc}G\left(G^TW_{acc}G\right)^{-1}G^TW_{acc}\right)y \quad (22)$$

In this equation, we have $W_{acc} = C_{acc}^{-1}$. The threshold is defined by:

$$F\left(T_{\chi^2}, n-3-N_{const}\right) = 1 - P_{FA\_CHI2} \quad (23)$$

In the above equation the operator $F(u, \deg)$ is the cdf of a chi-square distribution with *deg* degrees of freedom. If $\chi^2 > T_{\chi^2}$, but $\tau_{k,q} \leq 1$ for all q and k, the PL cannot be considered valid and exclusion cannot be attempted. In this case, the chi-square statistic is larger than expected, but none of the solution separation tests have failed, which suggests that the fault is outside the threat model. This test is a sanity check (a similar test is required for SBAS in [15]).

Results of this step: Thresholds $T_{k,q}$, decision on whether to continue with Protection Level calculation, attempt fault exclusion, or declare the HPL and VPL invalid.

Protection Levels

Vertical Protection Level (VPL)

The VPL is the solution to the equation:

$$2Q\left(\frac{VPL - b_3^{(0)}}{\sigma_3^{(0)}}\right) + \sum_{k=1}^{N_{fault\ modes}} p_{fault,k}Q\left(\frac{VPL - T_{k,3} - b_3^{(k)}}{\sigma_3^{(k)}}\right) = PHMI_{VERT}\left(1 - \frac{P_{sat,not\ monitored} + P_{const,not\ monitored}}{PHMI_{VERT} + PHMI_{HOR}}\right) \quad (24)$$

The output VPL must be within TOL_{PL} of the solution of this equation. There are several methods available to solve this equation. Appendix B proposes one of them, as well as a tight upper bound. The formal proof of safety associated to this Protection Level can be found in Appendix H.

Horizontal Protection Level (HPL)

For the HPL computations, we first compute HPL_q for q=1 and 2. HPL_q is the solution to the equation:

$$2Q\left(\frac{HPL_q - b_q^{(0)}}{\sigma_q^{(0)}}\right) + \sum_{k=1}^{N_{fault\ modes}} p_{fault,k}Q\left(\frac{HPL_q - T_{k,q} - b_q^{(k)}}{\sigma_q^{(k)}}\right) = \frac{1}{2}PHMI_{HOR}\left(1 - \frac{P_{sat,not\ monitored} + P_{const,not\ monitored}}{PHMI_{VERT} + PHMI_{HOR}}\right) \quad (25)$$

The output HPL_q must be within TOL_{PL} of the solution of this equation. This equation can be solved using a half interval search as shown for the VPL in Appendix B. The HPL is given by:

$$HPL = \sqrt{HPL_1^2 + HPL_2^2} \quad (26)$$

Results of this step: VPL and HPL

Accuracy, the fault free position error bound, and Effective Monitor Threshold

The standard deviation of the vertical position solution used for these two criteria is given by:

$$\sigma_{v,acc} = \sqrt{e_3^T S^{(0)} C_{acc} S^{(0)T} e_3} \quad (27)$$

The formulas for the two accuracy requirements are given by:

$$accuracy(95\%) = K_{ACC}\sigma_{v\_acc} \quad (28)$$

$$fault-free\left(10^{-7}\right) = K_{FF}\sigma_{v,acc} \quad (29)$$

Because 10 m / K_{FF} is smaller than 4 m / K_{ACC}, the fault-free test is the only one that needs to be evaluated by the aircraft.

The EMT takes into account the faults with a prior that is equal or larger than P_{EMT}. It is computed as follows:

$$K_{md,EMT,k} = Q^{-1}\left(\frac{P_{EMT}}{2p_{fault,k}}\right) \quad (30)$$

$$\sigma_{v,EMT}^{(k)} = \sqrt{e_3^T S^{(k)} C_{acc} S^{(k)T} e_3} \quad (31)$$

$$EMT = \max_{k|p_{faul,k} \geq P_{EMT}} \left(T_{k,3} + K_{md,EMT,k}\sigma_{v,EMT}^{(k)}\right) \quad (32)$$

Results of this step: 95% accuracy, the 10^{-7} fault free position error bound, and EMT

Fault exclusion

The objective of the fault exclusion function is twofold: to increase availability when there is little ambiguity as to which set of satellites is faulted, and to provide a notion of prior probability update.

Determination of candidates for exclusion

Fault exclusion is performed based on the test results $\tau_{k,q}$ from the solution separation tests. Fault exclusion is attempted when one of these test statistics has exceeded its threshold. If the all-in-view set is found to be inconsistent, the algorithm may have to exclude a subset of satellites of size N_{ex}. For each possible size N_{ex} of the subset we determine the best candidate for exclusion as follows:

$$k_{N_{ex}} = \arg\min_k \left\{\chi^{2(k)} \,|\, |idx_k| = N_{ex}\right\} \quad (33)$$

$$\chi^{2(k)} = y^T\left(W_{acc}^{(k)} - W_{acc}^{(k)}G\left(G^T W_{acc}^{(k)} G\right)^{-1} G^T W_{acc}^{(k)}\right)y \quad (34)$$

It will be shown below in Appendix F that the subset of satellites corresponding to this index is a good choice for exclusion with N_{ex} satellites. The candidate subsets are tested as explained below starting with N_{ex}=1. The search stops when a consistent set has been found (that is, when the tests described in the next paragraph pass). Notice that the search for a candidate set of size N_{ex} is performed among all possible subsets out of the all-in-view set.

Testing the candidate subsets

Let us suppose that we exclude the satellites corresponding to the k_{ex} subset. First, we determine a new position solution:

$$\Delta\hat{x}^{(0),new} = \left(G_{new}^T W_{new} G_{new}\right)^{-1} G_{new}^T W_{new} \Delta PR_{new} \quad (35)$$

The new set of measurements is obtained from the all-in-view by removing the pseudoranges in the k_{ex} subset. Following the same procedure as for the all-in-view we determine, $p_{fault,new,k}$,$idx_{,new,k}$ for k ranging from 0 to the maximum number of faults, $P_{sat,notmonitored,new}$, and $P_{const,not monitored,new}$

Similarly, we compute $\sigma_q^{(k)new}$, $\sigma_{ss,q}^{(k)new}$, $b_q^{(k)new}$ for k from 1 to $N_{faults,new}$, and from q from 1, 2, and 3. The solution separation tests are performed as before with the new thresholds $T_{k,q,new}$ (which are computed using Equation (18) using the appropriate subsets). To compute a Protection Level, these tests must pass.

Exclusion test to account for wrong exclusion probability

In addition to the previous tests, for each of the subsets we perform the following test. Let us consider the subset corresponding to $idx_{new,k}$. We consider the solution position from the all-in-view set that excludes the satellites that are not considered in $idx_{new,k}$, but that includes the satellites that were excluded in the previous step.

For example, let us suppose that there are six satellites: 1, 2, 3, 4, 5 and 6. Let us assume that 1 is excluded. Then the sets $idx_{new,k}$ would be (supposing one fault at a time): [3 4 5 6], [2 4 5 6], [2 3 5 6], [2 3 4 6], [2 3 4 5]. The corresponding indices $idx_{new,k}$ are the same to which we add the excluded satellite to obtain the following sets: [1 3 4 5 6], [1 2 4 5 6], [1 2 3 5 6], [1 2 3 4 6], [1 2 3 4 5]. Let us label k' the corresponding index. For each value of q we test:

$$\left|\hat{x}_q^{(k')} - \hat{x}_q^{(k)new}\right| > T_{k,q,exclusion} \tag{36}$$

Note that the position solutions corresponding to $idx_{k'}$ have already been computed for the faults deriving from independent satellite faults. They have not been computed when $idx_{k'}$ corresponds to the exclusion of a whole constellation. Note that in some of these cases, the above test will always fail, because both the left side and right side in the inequality are zero.

The threshold is computed as follows:

$$\sigma_{ss,q}^{(k,new-k')2} = \left(S_{q,.}^{(k)new} - S_{q,.}^{(k')}\right) C_{acc} \left(S_{q,.}^{(k)new} - S_{q,.}^{(k')}\right)^T \tag{37}$$

$$T_{k,q,exclusion} = Q^{-1}\left(\frac{p_{fault,k_{ex}}}{2}\right)\sigma_{ss,q}^{(k,new-k')} \tag{38}$$

We now define:

$$\begin{aligned} &\theta_k = 1 \text{ if } \left|\hat{x}_q^{(k')} - \hat{x}_q^{(k)new}\right| \le T_{k,q,exclusion} \text{ for all } q \\ &\theta_k = 0 \text{ otherwise} \end{aligned} \tag{39}$$

A value of $\theta_k = 1$ indicates that there is an increased risk that the wrong satellite has been excluded, as the subset under consideration appears to be consistent while it includes the excluded satellite. That means that another candidate for exclusion is present and this will have to be accounted for in the protection level computations after exclusion.

Protection Level computation after exclusion

After exclusion of the subset corresponding to the k^{th} index, the Protection Level equation is:

$$\begin{aligned} &2Q\left(\frac{VPL_{exclusion} - b_3^{(0),new}}{\sigma_3^{(0),new}}\right) p_{fault,k_{ex}}^{-\theta_0} + \\ &\sum_{k=1}^{N_{fault\ modes,new}} p_{fault,k,new} Q\left(\frac{VPL_{exclusion} - T_{k,3,new} - b_3^{(k)new}}{\sigma_3^{(k)new}}\right) p_{fault,k_{ex}}^{-\theta_k} \\ &= PHMI_{VERT}\left(1 - \frac{P_{sat,not\ monitored,new} + P_{const,not\ monitored,new}}{PHMI_{VERT} + PHMI_{HOR}}\right) \end{aligned} \tag{40}$$

This equation is formally identical to the PL equation for the all-in-view. There is however a difference: each term has the additional factor $p_{fault,k_{ex}}^{-\theta_k}$ ($p_{fault,k_{ex}}$ is, we recall, the probability of fault mode k_{ex} in the original list of faults). As will be seen below, the addition of this factor guarantees that the integrity risk given the test results is below the requirements.

This term can also be interpreted as follows: If the exclusion test passes (that is, it exceeds the threshold) it means that the subset under consideration confirms that the proposed excluded satellite (or group of satellites) appears to be faulty. If the test doesn't pass, it means that the subset of satellites that was excluded is itself a suspect. We therefore need to increase its prior probability.

Accuracy computation after exclusion

Because the prior probability might be modified if the test doesn't pass, fault modes need to be taken into account when computing the 95% error bound, which we label $VPE_{95\%}$. We need to have:

$$\begin{aligned} &2Q\left(\frac{VPE_{95\%} - b_3^{(0),new}}{\sigma_3^{(0),new}}\right) p_{fault,k_{ex}}^{-\theta_0} + \\ &\sum_{k=1}^{N_{faults\ modes,new}} p_{fault,k,new} Q\left(\frac{L_{95\%} - T_{k,3,new} - b_3^{(k)new}}{\sigma_3^{(k)new}}\right) p_{fault,k_{ex}}^{-\theta_k} = 95\% \end{aligned} \tag{41}$$

Integrity of the exclusion algorithm

The probability of HMI given the test results can be developed as follows:

$$P\left(HMI \mid \text{test results}\right) = \frac{P\left(HMI, \text{test results}\right)}{P\left(\text{test results}\right)} \tag{42}$$

The exclusion of the satellites in subset k_{ex} can be attempted if we have:

$$\max_q \tau_{k_{ex},q} \geq 1 \tag{43}$$

The exclusion tests provide the additional conditions θ_k. These conditions do not affect the decision to exclude, but they do affect the calculation of the Protection Levels.

We first compute an estimate of the event labeled "test results(θ)":

$$\text{test results}\left(\theta\right) = \left\{\max_q \tau_{k_{ex},q} \geq 1, \max_{k,q} \tau_{k,q,new} \leq 1, \Theta_k = \theta_k\right\} \tag{44}$$

The first condition states that the subset k_{ex} has exceeded the threshold. The second condition states that after excluding this subset, the solution separation tests pass. Finally, the third set of tests (the exclusion tests) checks whether each separate subset confirms the exclusion of k_{ex}. It is not possible to compute the exact probability of this event, because faults can produce any bias in the measurements. However, we can say that this set of test results is very likely to happen if the subset k_{ex} is indeed faulty. It is therefore reasonable to assume that:

$$\begin{aligned}&\mathrm{P}\left(\text{test results}\right) = \\ &\mathrm{P}\left\{\max_q \tau_{k_{ex},q} \geq 1, \max_{k,q} \tau_{k,q,new} \leq 1, \Theta_k = \theta_k\right\} \sim p_{fault,k_{ex}}\end{aligned} \tag{45}$$

That is, the probability of obtaining these test results is on the order of the probability of having a fault in the subset k_{ex}.

We now evaluate the probability:

$$\begin{aligned}&P\left(HMI, \text{test results}\right) = \\ &P\left(\begin{array}{l}\left|x_q - \hat{x}_q^{(k_{ex})}\right| > VPL_{k_{ex}}, \forall k \left|x_q^{(k)new} - \hat{x}_q^{(k_{ex})}\right| \\ \leq T_{k,q,new}, \left|\hat{x}_q^{(k')} - \hat{x}_q^{(k)new}\right| \geq \left(1-\theta_k\right) T_{k,q,exclusion}\end{array}\right)\end{aligned} \tag{46}$$

We have the approximate inequality:

$$\begin{aligned}&P\left(HMI, \text{test results}\left(\theta\right) \mid \text{fault } k\right) \leq \\ &P\left(\left|x_q - \hat{x}_q^{(k)new}\right| > VPL_{k_{ex}} - T_{k,q,new} \mid \text{fault } k\right) \times \\ &P\left(\left|\hat{x}_q^{(k')} - \hat{x}_q^{(k)new}\right| \geq \left(1-\theta_k\right) T_{k,q,exclusion} \mid \text{fault } k\right) \\ &\simeq P\left(\left|x_q - \hat{x}_q^{(k)new}\right| > VPL_{k_{ex}} - T_{k,q,new} \mid \text{fault } k\right) p_{fault,k_{ex}}^{1-\theta_k} \\ &= Q\left(\frac{VPL_{exclusion} - T_{k,3,new} - b_3^{(k)new}}{\sigma_3^{(k)new}}\right) p_{fault,k_{ex}}^{1-\theta_k}\end{aligned} \tag{47}$$

This inequality shows that if the post-exclusion VPL is computed according to (40) then the integrity requirement integrity is met given the test results, if it is assumed that the neglected fault modes are negligible.

Result of this step: Index of faulted satellites or constellations, post-exclusion VPL and HPL

Monitoring previously excluded satellites (preliminary)

Satellites previously excluded must be monitored every T_{CHECK}. This is done by comparing the measured range to the expected range. The expected range $PR_{expected}$ is based on the position and clock solution using the healthy satellites. The excluded satellite can only be included in the solution once it has passed a threshold test for the last T_{RECOV}. The threshold test is not yet defined.

Result of this step: consistency of previously excluded satellites (flags)

4. LIST OF POSSIBLE REFINEMENTS TO THE BASELINE ALGORITHM

In this section we briefly describe possible improvements of the reference algorithm that were considered and studied to varying degrees by the ARAIM subgroup. These changes can be classified by where they differ from the reference algorithm.

Improvements in the false alert risk allocation among modes

In the baseline algorithm, the false alert allocation is split evenly across all fault modes. As explained in [12], there is an optimal choice of false alert allocation that could reduce both the PLs and the EMT. In [6] the false alert allocation was chosen to minimize all thresholds. This approach works when all thresholds are considered in the EMT calculation, but can result in higher PLs and EMT if it is not the case. Since the constellation faults are the dominant terms in the EMT, an approach where the false alert allocation is mostly given to the constellation fault modes would be a good choice (and probably close to the optimal choice given in [12]).

Another way to improve the false alert allocation is by taking into account that some tests are actually redundant. For example, in the one satellite out case the solution separation tests in each coordinate are measuring the same statistic.

Improvements in the calculation of the Protection Level

The Protection Level above may be reduced by refining the calculation of the integrity risk. A description of this approach can be found in [16]. In the baseline algorithm, the upper bound of the contribution is used:

$$P\left(HMI \mid \text{fault } k\right) \leq Q\left(\frac{VPL - T_{k,3} - b_3^{(k)}}{\sigma_3^{(k)}}\right) \quad (48)$$

In this proposed change, a finer upper bound is defined as a function of two parameters instead of one:

$$P\left(HMI \mid \text{fault } k\right) \leq F\left(\frac{VPL - T_{k,3} - b_3^{(k)}}{\sqrt{\sigma_3^{(k)2} - \sigma_3^{(0)2}}}, \frac{\sigma_3^{(0)}}{\sqrt{\sigma_3^{(k)2} - \sigma_3^{(0)2}}}\right) \quad (49)$$

The function F is defined as:

$$F(\gamma, \rho) = \max_u Q(u) Q\left(\sqrt{1+\rho^2}\gamma - \rho u\right) \quad (50)$$

A derivation of Equation (49) can be found in Appendix K. The Protection Level is then the solution of the modified equation:

$$2Q\left(\frac{VPL - b_3^{(0)}}{\sigma_3^{(0)}}\right) + \sum_{k=1}^{N_{fault\ modes}} p_{fault,k} F\left(\frac{VPL - T_{k,3} - b_3^{(k)}}{\sqrt{\sigma_3^{(k)2} - \sigma_3^{(0)2}}}, \frac{\sigma_3^{(0)}}{\sqrt{\sigma_3^{(k)2} - \sigma_3^{(0)2}}}\right) = PHMI_{VERT}\left(1 - \frac{P_{sat,not\ monitored} + P_{const,not\ monitored}}{PHMI_{VERT} + PHMI_{HOR}}\right) \quad (51)$$

A similar idea is exploited in the Q-method [17]. In the Q-method, a two dimensional function, or map, is pre-computed. For a given probability of misdetection, this map provides the PL as a function of two parameters related to the geometry.

Threat model modifications

The threat model can be refined by limiting the potential effect of constellation-wide faults [18], [19]. Constellation-wide faults caused by erroneous EOP/EOPPs would mostly affect the position error in the horizontal plane, and in a consistent way. This constraint can be expressed by writing that a fault mode is the addition of a nuisance parameter b_{EOP}. The measurement model in the faulted case is given by:

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} G_1 & 0 \\ G_2 & \tilde{G}_2 \end{bmatrix} \begin{bmatrix} x \\ b_{EOP} \end{bmatrix} + n \quad (52)$$

In this equation y_i is the vector of measurements from constellation i. The variable x is the actual position and clock offsets. The matrix $[G_1^T\ G_2^T]^T$ is the matrix G defined above. $\tilde{G}_2$ is defined by:

$$\tilde{G}_2 = G_2 \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}^T \quad (53)$$

If only the East West coordinate is affected then:

$$\tilde{G}_2 = G_2 \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix}^T \quad (54)$$

This modified constellation fault can be handled either with a chi-square approach as outlined in [18], or within the framework of the reference solution separation algorithm [20], by computing a position solution tolerant to this fault. The algorithm then proceeds identically. It is possible to relax the constraint that the error only affects the horizontal coordinates by allowing the vertical position error due to the fault to be non-zero, but by bounding its magnitude by the magnitude of the error in the horizontal plane [21]. These approaches are very appealing because they lessen the effect of constellation wide faults on availability, to the point where they barely affect it. However, it is not known to the subgroup at this time whether it can be assumed that the vertical error caused by constellation wide faults is always no larger than the horizontal errors. Additionally, it is not clear that EOP/EOPP faults can only affect one constellation at a time

Ground validated long term ephemeris for EOP fault mitigation

As in the previous section, the objective of this proposed improvement is to mitigate the effect of constellation wide faults. The idea consists of sending to the user a validated source for the computation of satellite position, which can either be used directly in the positioning process or for detection of faults in the current broadcast ephemerides. A method of the second type, which is directly applicable to the detection of EOP/EOPP faults, is described in [22]. The method uses adjacent ephemerides to detect EOP/EOPP faults introduced at ephemeris data set cutovers. It is significant that this method, unlike the ARAIM methods described in the sections above, *does not depend on independence of EOP/EOPP faults across GNSS core constellations.* The drawback is that EOP/EOPP faults that are solely growing relative to the specified GPS fault exposure limit of 6 hours [23] cannot be reliably detected using adjacent ephemeris tests. An alternative method, based on long-term projection of validated ephemerides is briefly introduced in [24] and is currently being investigated. Related methods have exhibited good performance for long-term orbit propagation in mobile phone positioning applications [25]. The role of the ARAIM ground segment (which determines the ISM) would be to create projection model parameters using a series of previously ground-validated ephemerides. Using auxiliary methods like these to eliminate EOP/EOPP faults would allow the receiver ARAIM algorithms to assume a very low probability of constellation fault P_{const}, and it would alleviate the need to prove independence of EOP/EOPP faults across constellations. Such methods would also be effective in a single constellation reversionary mode.

Improvements in the position solution

The reference algorithm computes an all-in-view position solution based on a least squares approach using C_{int} as the covariance of the pseudorange errors. The Protection Level may be reduced by choosing a different position solution. This approach has been exploited in NIORAIM within the framework of slope-based RAIM, where single faults are assumed [26] and accuracy constraints are not considered. It has also been exploited in OWAS, which considers both accuracy and integrity constraints [27].

It is possible to simultaneously optimize the integrity allocation and the position solution, take into account additional constraints when generating the position solution - for example the accuracy, but not only -, and do it for any threat model (in particular multiple faults). This is done by casting the problem as a convex optimization problem. The algorithm is described in [28]. To illustrate the algorithm, we rewrite the Vertical Protection Level equation to make the threshold explicit:

$$
\begin{aligned}
&2Q\left(\frac{VPL-b_3^{(0)}}{\sigma_3^{(0)}}\right)+\\
&\sum_{k=1}^{N_{fault\ modes}} p_{fault,k} Q\left(\frac{VPL-K_{fa,3}\sqrt{\left(S_{3,\cdot}^{(k)}-S_{3,\cdot}^{(0)}\right)C_{acc}\left(S_{3,\cdot}^{(k)}-S_{3,\cdot}^{(0)}\right)^T}-b_3^{(k)}}{\sigma_3^{(k)}}\right)\\
&=PHMI_{VERT}\left(1-\frac{P_{sat,not\ monitored}+P_{const,not\ monitored}}{PHMI_{VERT}+PHMI_{HOR}}\right)
\end{aligned}
\tag{55}
$$

The approach consists on modifying the all-in-view position solution coefficients so that the VPL is minimized (that is, $S_{3,\cdot}^{(0)}$ is no longer calculated using a weighted least-squares) while meeting the accuracy and EMT constraints.

Test simplification

It is possible to bypass the computation of all subsets positions at the expense of a slightly degraded performance. We have the inequality (where W_{acc} is the inverse of C_{acc}):

$$
\begin{aligned}
&\left|\Delta\hat{x}_q^{(k)}\right|^2=\left|\hat{x}_q^{(k)}-\hat{x}_q^{(0)}\right|^2\leq\\
&\sigma_{ss,q}^{(k)\,2}\left(y^T\left(W_{acc}-W_{acc}G\left(G^TW_{acc}G\right)^{-1}G^TW_{acc}\right)y\right)
\end{aligned}
\tag{56}
$$

The only test to be performed is to check whether:

$$
\begin{aligned}
&y^T\left(W_{acc}-W_{acc}G\left(G^TW_{acc}G\right)^{-1}G^TW_{acc}\right)y\\
&\leq T_{\chi^2,alternate}={\chi^2_{n-3-N_{const}}}^{-1}\left(1-P_{FA}\right)
\end{aligned}
\tag{57}
$$

If the test passes, the Protection Levels are computed taking:

$$T_{k,q} = \sigma_{ss,q}^{(k)} \sqrt{T_{\chi^2, alternate}} \qquad (58)$$

More details on this simplification can be found in Appendix F.

SUMMARY

This work presents a step by step specification of a baseline Advanced RAIM airborne algorithm which is multi-constellation capable and can protect against a multiple fault threat model. The algorithm is based on solution separation, because it makes the treatment of multiple faults simple, and because it is shown to be optimal in a certain sense. The key steps in the calculation of the availability criteria (VPL, HPL, EMT and accuracy) are: the determination of the fault modes to be monitored based on the contents of the ISM, the computation of the subset position solutions as well as their corresponding standard deviations, and the solution of the Protection Level equations. Then, we describe an exclusion algorithm that meets the integrity requirements given that exclusion is attempted that is not computationally intensive. As this algorithm requires the computation of a potentially large number of position solutions, we indicate how the computation of subset position solutions can be made very efficient with the use of rank one update formulas. Finally, we summarize several possible improvements that were not included in the current baseline algorithm.

ACKNOWLEDGEMENTS

The authors wish to thank all the members of the WG-C ARAIM subgroup (of which the authors list is a subset). For the U.S. authors, this research was sponsored by the F.A.A.

APPENDIX A

Error Models

Two error budgets for GPS and Galileo have been made use of to allow for a performance prediction in the frame of ARAIM. The Galileo user contribution to the error budget is identified in tabular form.

(meters)	Galileo			
	5°	0.4529m	50°	0.2359 m
	10°	0.3553 m	55°	0.2339 m
	15°	0.3063 m	60°	0.2302 m
$\sigma_{n,user}^{Gal}$	20°	0.2638 m	65°	0.2295 m
	25°	0.2593 m	70°	0.2278 m
(vs elevation)	30°	0.2555 m	75°	0.2297 m
	35°	0.2504 m	80°	0.2310 m
	40°	0.2438 m	85°	0.2274 m
	45°	0.2396 m	90°	0.2277 m

Table A-1. Galileo Elevation Dependent SIS user error

The $\sigma_{n,user}$ for GPS follows the formula provided in [29] for the Airborne Accuracy Designator – Model A (AAD-A) [30]:

$$\sigma_{n,user}^{GPS} = \sqrt{\frac{f_{L1}^4 + f_{L5}^4}{\left(f_{L1}^2 - f_{L5}^2\right)^2}} \sqrt{\left(\sigma_{MP}\right)^2 + \left(\sigma_{Noise}\right)^2}$$

$$\sigma_{MP}(\theta) = 0.13[\mathrm{m}] + 0.53[\mathrm{m}]\exp(-\theta/10[\deg])$$

$$\sigma_{Noise}(\theta) = 0.15[\mathrm{m}] + 0.43[\mathrm{m}]\exp(-\theta/6.9[\deg]) \qquad (59)$$

where θ is the elevation angle in degrees. This represents an overbound of the error after carrier smoothing.

The tropospheric delay $\sigma_{n,tropo}$ can be modeled according to [31] as

$$\sigma_{n,tropo}(\theta) = 0.12[\mathrm{m}] \frac{1.001}{\sqrt{0.002001 + \left(\sin\left(\frac{\pi\theta}{180}\right)\right)^2}} \qquad (60)$$

where θ is given in degrees and relates to the elevation angle.

APPENDIX B

Method to Solve the VPL Equation

The VPL can be obtained by solving the following equation using a half interval search:

$$P_{exceed}\left(VPL\right) = PHMI_{VERT,ADJ} \tag{61}$$

where:

$$P_{exceed}\left(VPL\right) = 2Q\left(\frac{VPL - b_3^{(0)}}{\sigma_3^{(0)}}\right) + \sum_{k=1}^{N_{fault\ \mathrm{modes}}} p_{fault,k}\, Q\left(\frac{VPL - T_{k,3} - b_3^{(k)}}{\sigma_3^{(k)}}\right) \tag{62}$$

and:

$$PHMI_{VERT,ADJ} = PHMI_{VERT}\left(1 - \frac{P_{sat,not\ monitored} + P_{const,not\ monitored}}{PHMI_{VERT} + PHMI_{HOR}}\right) \tag{63}$$

This search can be started with the lower and upper bounds which relate to full and even allocation of the integrity risk respectively and are given by:

$$VPL_{low,init} = \max\left\{\begin{aligned} & Q^{-1}\left(\frac{PHMI_{VERT,ADJ}}{2}\right)\sigma_3^{(0)} + b_3^{(0)}, \\ & \max_k Q^{-1}\left(\frac{PHMI_{VERT,ADJ}}{p_{fault,k}}\right)\sigma_3^{(k)} + T_{k,3} + b_3^{(k)} \end{aligned}\right\} \tag{64}$$

$$VPL_{up,init} = \max\left\{\begin{aligned} & Q^{-1}\left(\frac{PHMI_{VERT,ADJ}}{2\left(N_{faults}+1\right)}\right)\sigma_3^{(0)} + b_3^{(0)}, \\ & \max_k Q^{-1}\left(\frac{PHMI_{VERT,ADJ}}{p_{fault,k}\left(N_{faults}+1\right)}\right)\sigma_3^{(k)} + T_{k,3} + b_3^{(k)} \end{aligned}\right\} \tag{65}$$

The iterations stop when:

$$\left|VPL_{up} - VPL_{low}\right| \le TOL_{PL} \tag{66}$$

The final VPL is given by VPL_{up} at the end of iteration. In the case of HPL_1 and HPL_2, the approach is identical, but the appropriate parameters must be changed.

Approximation Not Requiring an Iterative Algorithm

The function P_{exceed} is convex so a linear approximation provides a tight upper bound of the VPL:

$$\begin{aligned} VPL_{approx,upper} &= VPL_{low,init} + \\ & \left(PHMI_{VERT} - P_{exceed}\left(VPL_{low,init}\right)\right)\times \\ & \frac{VPL_{upper,init} - VPL_{low,init}}{P_{exceed}\left(VPL_{upper,init}\right) - P_{exceed}\left(VPL_{low,init}\right)} \end{aligned} \tag{67}$$

Similarly, the function log P_{exceed} is concave, so a linear approximation provides a tight lower bound:

$$\begin{aligned} VPL_{approx,low} &= VPL_{low,init} + \\ & \left(\log PHMI_{VERT,ADJ} - \log P_{exceed}\left(VPL_{low,init}\right)\right)\times \\ & \frac{VPL_{upper,init} - VPL_{low,init}}{\log P_{exceed}\left(VPL_{upper,init}\right) - \log P_{exceed}\left(VPL_{low,init}\right)} \end{aligned} \tag{68}$$

APPENDIX C

Algorithm That Determines the Maximum Size of the Subsets That Need to Be Monitored and the Contribution to the Integrity Budget of All Unmonitored Subsets

Probability of subset fault

In the following equations, $p_{sat,i}$ is the prior probability of fault in satellite i, which is included in the Integrity Support Message (and are not necessarily identical). The probability that the set of satellites $i_1, i_2, \ldots, i_r$ is faulty, and the remaining ones are not faulty is given by:

$$\begin{aligned} & \prod_{s=1,\cdots,r} p_{sat,i_s} \prod_{s\neq 1,\cdots,r}\left(1 - p_{sat,i_s}\right) = \\ & \prod_{k=1}^{N_{sat}}\left(1 - p_{sat,k}\right) \prod_{s=1,\cdots,r} \frac{p_{sat,i_s}}{1 - p_{sat,i_s}} \\ & = p_{no\_fault} \prod_{s=1,\cdots,r} \frac{p_{sat,i_s}}{1 - p_{sat,i_s}} \end{aligned} \tag{69}$$

where:

$$p_{no\_fault} = \prod_{k=1}^{N_{sat}}\left(1 - p_{sat,k}\right) \tag{70}$$

This probability is bounded by the probability that the set of satellites $i_1, i_2, \ldots, i_r$ is faulty, and the remaining ones are either faulty or not, which is given by:

$$\prod_{s=1}^{r} p_{sat,i_s} \quad (71)$$

Probability that r or more satellites are faulted

For *r = 1, r =2, and r=3*, the exact probability can be easily computed.

The probability that there are 1 or more faults is given by:

$$1 - p_{no\_fault} \quad (72)$$

The probability that there are 2 or more faults is given by:

$$1 - p_{no\_fault} - p_{no\_fault} \sum_{i_1=1}^{N_{sat}} \frac{p_{sat,i_1}}{1 - p_{sat,i_1}} \quad (73)$$

The probability that there are 3 or more simultaneous faults is given by:

$$1 - p_{no\_fault} \left(1 + \sum_{i_1=1}^{N_{sat}} \frac{p_{sat,i_1}}{1 - p_{sat,i_1}} \right) - p_{no\_fault} \sum_{i_1 < i_2} \frac{p_{sat,i_1}}{1 - p_{sat,i_1}} \frac{p_{sat,i_2}}{1 - p_{sat,i_2}} \quad (74)$$

The probability that *r* or more satellites are faulted is smaller than:

$$P_{sat\_subsets}\left(r, p_{sat,1}, \cdots, p_{sat,N_{sat}}\right) \leq \sum_{i_1 < i_2 < \cdots < i_r} \prod_{i_1, i_2, \cdots, i_r} p_{sat,i_j} = \sum_{i_1 < i_2 < \cdots < i_r} p_{sat,i_1} \cdots p_{sat,i_r} \quad (75)$$

The formula increases in complexity with *r*. An upper bound is given by:

$$P_{sat\_subsets}\left(r, p_{sat,1}, \cdots, p_{sat,N_{sat}}\right) = \sum_{i_1 < i_2 < \cdots < i_r} p_{sat,i_1} \cdots p_{sat,i_r} \leq \frac{\left(\sum_{k=1}^{N_{sat}} p_{sat,k} \right)^r}{r!} \quad (76)$$

This upper bound can be shown by considering the development of the right term and noticing that the left term is a subset of the resulting terms.

Determination of $N_{sat,max}$

Using Equation (76), $N_{sat,max}$ can be determined by:

$$N_{sat,\max} = \varphi_{P_{SAT\_THRES}} \left(\sum_{k=1}^{N_{sat}} p_{sat,k} \right) \quad (77)$$

$\varphi_{P_{SAT\_THRES}}$ is defined by:

$$\varphi_{P_{SAT\_THRES}}(u) = \min \left\{ r \mid \frac{u^{r+1}}{(r+1)!} \leq P_{SAT\_THRES} \right\} \quad (78)$$

With this definition, we have:

$$\begin{aligned} &\varphi_{P_{SAT\_THRES}}(u) = 0 \text{ for } u \leq P_{SAT\_THRES} \\ &\varphi_{P_{SAT\_THRES}}(u) = 1 \text{ for } P_{SAT\_THRES} < u \leq \left(2P_{SAT\_THRES}\right)^{\frac{1}{2}} \\ &\varphi_{P_{SAT\_THRES}}(u) = 2 \text{ for } \left(2P_{SAT\_THRES}\right)^{\frac{1}{2}} < u \leq \left(6P_{SAT\_THRES}\right)^{\frac{1}{3}} \end{aligned} \quad (79)$$

More generally:

$$\varphi_{P_{SAT\_THRES}}(u) = r \text{ for } \left(r!P_{SAT\_THRES}\right)^{\frac{1}{r}} < u \leq \left((r+1)!P_{SAT\_THRES}\right)^{\frac{1}{r+1}} \quad (80)$$

Example of minimum subset size

The table below shows the minimum number of simultaneous satellite faults that need to be tested as a function of P_{sat} (assuming it is the same for all satellites) and N_{sat}. For example, for 35 satellites and a prior of 5×10^{-4}, the total probability of fault of the subsets with more 4 satellites or more is below the threshold P_{SAT_THRES}, and only subsets with 1, 2 or 3 faults need to be taken into account.

P_{sat}/N_{sat}	10	15	20	25	30	35	40
10^{-5}	1	1	1	1	2	2	2
10^{-4}	2	2	2	2	2	2	2
5×10^{-4}	2	3	3	3	3	3	3
10^{-3}	3	3	3	3	3	4	4

Table C1. $N_{sat,max}$ as a function of P_{sat} and N_{sat}

Probability that p or more constellations are faulted

We define:

$$p_{no\_const\_fault} = \prod_{k=1}^{N_{const}} \left(1 - p_{const,k}\right) \quad (81)$$

The probability that there are 1 or more constellation faults is given by:

$$P_{const\_subsets}\left(1, p_{const,1}, \cdots, p_{const,N_{const}}\right) = 1 - p_{no\_const\_fault} \quad (82)$$

The probability that there are 2 or more constellation faults is given by:

$$\begin{aligned} &P_{const\_subsets}\left(1, p_{const,1}, \cdots, p_{const,N_{const}}\right) = \\ &1 - p_{no\_const\_fault} - p_{no\_const\_fault} \sum_{k=1}^{N_{const}} \frac{p_{const,k}}{1 - p_{const,k}} \end{aligned} \quad (83)$$

APPENDIX D

Additional Considerations on Subset Determination

It is possible to reduce the number of subsets to be tested by including smaller subsets in larger ones. For example, a multiple satellite fault of satellites belonging to the same constellation can be counted by increasing the prior of the constellation fault. As an example, for *n* satellites of a same constellation with a prior of p_{sat}, and where it has been determined that all subsets with two satellites must be tested, it is possible to only test the constellation wide fault provided that p_{const} is changed as follows:

$$p_{const,adjusted} = p_{const} + \binom{n}{2} p_{sat}^2 \quad (84)$$

It is still necessary to check all subsets of two satellites where each belongs to a different constellation.

APPENDIX E

Relationship between Chi-square and Solution Separation

Link to Parity Vector and Chi-square based RAIM Methods

In addition to simplifying the processing, the variant expressed by Equation (58) highlights the link of the proposed algorithm with other RAIM approaches. This link becomes more apparent with the following relationship [12]:

$$\sigma_{ss,3}^{(i)} = Vslope,i \quad (85)$$

Here *Vslope,i* is defined as the ratio of the vertical position error over the square root of the chi-square statistic assuming that all satellites have zero error except the i^{th} one.

Proof of the inequality (56)

The proof of this inequality is as follows. We have:

$$\left|\Delta\hat{x}_q^{(k)}\right|^2 = \left|\hat{x}_q^{(k)} - \hat{x}_q^{(0)}\right|^2 = \left|\left(S_{q,\cdot}^{(k)} - S_{q,\cdot}^{(0)}\right) W_{acc}^{-\frac{1}{2}} W_{acc}^{+\frac{1}{2}} \left(y - Gx\right)\right|^2$$

for any x

(86)

Applying the Cauchy-Schwarz inequality, we have:

$$\begin{aligned} &\left|\hat{x}_q^{(k)} - \hat{x}_q^{(0)}\right|^2 = \left|\left(S_{q,\cdot}^{(k)} - S_{q,\cdot}^{(0)}\right) W_{acc}^{-\frac{1}{2}} W_{acc}^{\frac{1}{2}} \left(y - Gx\right)\right|^2 \\ &\le \left|\left(S_{q,\cdot}^{(k)} - S_{q,\cdot}^{(0)}\right) W_{acc}^{-\frac{1}{2}}\right|^2 \left|W_{acc}^{\frac{1}{2}} \left(y - Gx\right)\right|^2 \end{aligned} \quad (87)$$

The first term in the product is given by:

$$\left|\left(S_{q,\cdot}^{(k)} - S_{q,\cdot}^{(0)}\right) W_{acc}^{-\frac{1}{2}}\right|^2 = \sigma_{ss,q}^{(k)\,2} \quad (88)$$

The second term is equal to:

$$\left|W_{acc}^{\frac{1}{2}} \left(y - Gx\right)\right|^2 = \left(y - Gx\right)^T W_{acc} \left(y - Gx\right) \quad (89)$$

Because this is true for any x, we can take the minimum of the above expression, which is:

$$\begin{aligned} &\min_x \left(y - Gx\right)^T W_{acc} \left(y - Gx\right) = \\ &y^T \left(W_{acc} - W_{acc} G \left(G^T W_{acc} G\right)^{-1} G^T W_{acc}\right) y \end{aligned} \quad (90)$$

APPENDIX F

Proof that Subset That Minimizes Its Chi-square Statistic Is a Good Choice for Exclusion

For this Appendix, we assume that W_{acc} and W_{int} coincide. We show that the subset with the largest solution separation residual is a good choice for exclusion. As shown in Appendix F, we have:

$$\left|\frac{\hat{x}_q^{(k)} - \hat{x}_q^{(0)}}{\sigma_{ss,q}^{(k)}}\right|^2 \le y^T \left(W_{acc} - W_{acc} G\left(G^T W_{acc} G\right)^{-1} G^T W_{acc}\right) y = \chi_{acc}^2 \tag{91}$$

This means that the subset that minimizes its chi-square statistic is a good choice for exclusion, because the chi-square statistic is an upper bound of the solution separation test ratio.

In the case of one satellite exclusion, we have the following relationship (see Appendix I):

$$\begin{aligned}\chi^2 &= \chi_{\hat{i}}^2 + \frac{w_i\left(y_i - g^T\left(G_{\hat{i}}^T W_{\hat{i}} G_{\hat{i}}\right)^{-1} G_{\hat{i}}^T W_{\hat{i}} y_{\hat{i}}\right)^2}{1 + g^T w_i \left(G_{\hat{i}}^T W_{\hat{i}} G_{\hat{i}}\right)^{-1} g} \\ &= \chi_{\hat{i}}^2 + \left(\frac{\hat{x}_q^{\hat{i}} - \hat{x}_q^{(0)}}{\sigma_{ss,q}^{\hat{i}}}\right)^2\end{aligned} \tag{92}$$

$\chi_{\hat{i}}^2$ is the chi-square statistic computed without satellite i. We therefore see that to minimize the chi-square statistic we must maximize the normalized solution separation (in the case of one satellite exclusion).

APPENDIX G

Optimality of the Solution Separation Test under Certain Conditions

We give elements of the proof that in the case of Gaussian noise, the test that minimizes the integrity risk at a constant probability of false alert is the solution separation test. Under no fault, we have the measurement equation:

$$y = Gx + \varepsilon \tag{93}$$

A fault can be defined by the effect it has on the measurement equation:

$$y = Gx + \varepsilon + Ab \tag{94}$$

A is an n by m matrix and b an m by one vector. We solve the optimization problem (there are other forms of presenting the problem, but they are equivalent):

$$\begin{aligned}&\underset{\Omega}{\text{minimize}}\ \max_b\ \text{Prob}\left(\left|\hat{x}_3 - x_3\right| > VAL, y = Gx + \varepsilon + Ab \in \Omega\right) \\ &\text{such that Prob}\left(y = Gx + \varepsilon \notin \Omega\right) = P_{fa}\end{aligned} \tag{95}$$

That is, we wish to find the region Ω that meets the false alarm requirement and minimizes the integrity risk within the VAL. We show that the optimal region is defined by the solution separation between the all-in-view solution and the least-squares solution that is unaffected by the fault. The all-in-view solution is given by:

$$\begin{aligned}\hat{x} &= Sy \\ S &= \left(G^T WG\right)^{-1} G^T W\end{aligned} \tag{96}$$

The first step consists on a change of variable. We define:

$$\begin{aligned}&\begin{bmatrix}\hat{x}_A \\ \hat{b}\end{bmatrix} = \begin{bmatrix}G^T WG & G^T WA \\ A^T WG & A^T WA\end{bmatrix}^{-1} \begin{bmatrix}G^T W \\ A^T W\end{bmatrix} y = \\ &\begin{bmatrix}\left(G^T WG\right)^{-1} + SAR^{-1}A^T S^T & -SAR^{-1} \\ -R^{-1}A^T S^T & R^{-1}\end{bmatrix}\begin{bmatrix}G^T W \\ A^T W\end{bmatrix} y \\ &P = I - G\left(G^T WG\right)^{-1} G^T W \\ &R = A^T WPA\end{aligned} \tag{97}$$

$\hat{x}_A$ is the least-squares solution unaffected by the fault. We do the change of variables:

$$y \to \hat{x}_A, \hat{b}, y - G\hat{x}_A - A\hat{b} \tag{98}$$

In this change of variables we have projected the vector of measurements onto the fault tolerant position estimate, the estimate of the fault bias, and the corresponding parity vector. The following formulas can be verified:

$$\begin{aligned}\hat{x}_A &= \hat{x} - SAR^{-1}A^T WPy \\ \hat{b} &= R^{-1}A^T WPy \\ y - \left(G\hat{x}_A + A\hat{b}\right) &= P\left(I - AR^{-1}A^T W\right) Py\end{aligned} \tag{99}$$

In the presence of a bias, the vertical position error is given by:

$$\begin{aligned}\hat{x}_3 - x_3 &= e_3^T Sy - x_3 \\ &= e_3^T S\left(\varepsilon + Ab\right) = e_3^T S\varepsilon + e_3^T SAb\end{aligned} \tag{100}$$

where:

$$e_3 = \begin{bmatrix}0 & 0 & 1 & 0 & 0\end{bmatrix}^T \tag{101}$$

The next step consists on determining which information in $\hat{x}_A, \hat{b}, y - G\hat{x}_A - A\hat{b}$ is relevant to the vertical position error. We have:

$$y-\left(G\hat{x}_A + A\hat{b}\right) = P\left(I - AR^{-1}A^TW\right)P\varepsilon \qquad (102)$$

The parity vector above does not depend on the vector *b*. In addition, as can be expected, the random component is uncorrelated from the random error in the position error:

$$\begin{aligned} &E\left(P\left(I-AR^{-1}A^TW\right)P\varepsilon\left(e_3^TS\varepsilon\right)^T\right) = \\ &P\left(I-AR^{-1}A^TW\right)PW^{-1}S^Te_3 = 0 \end{aligned} \qquad (103)$$

There is therefore no information in this parity vector about the vertical position error.

We now examine $\hat{x}_A$:

$$\hat{x}_A = x + S\varepsilon - SAR^{-1}A^TWP\varepsilon \qquad (104)$$

Since it is affected by the true position, which can be anything, there is no information on the position error in $\hat{x}_A$. This means, as was expected, that all the information is contained in $\hat{b}$. We now perform another change of variable:

$$\begin{aligned} &b_V = v^Tb \\ &v = \left(e_3^TSA\right)^T \\ &b_{other} = V^Tb \\ &V^Tv = 0 \end{aligned} \qquad (105)$$

The columns of V are orthogonal to v and complete v into a basis of R^m. We consider now the change of variables on the statistics:

$$\hat{b} \rightarrow v^T\hat{b}, V^T\hat{b} \qquad (106)$$

We have:

$$\hat{x}_3 - x_3 = e_3^TS\varepsilon + b_V \qquad (107)$$

Because the biases b are arbitrary, so are the components of the vector $[b_V \;\; b_{other}^T]^T$. Therefore, there is no information on the position error in the variable:

$$V^T\hat{b} = b_{other} + V^TR^{-1}A^TWP\varepsilon \qquad (108)$$

This means that all the information is in the scalar random variable $v^T\hat{b}$. We have:

$$v^T\hat{b} = e_3^TSA\hat{b} = e_3^TSAR^{-1}A^TWPy = e_3^T\left(\hat{x}-\hat{x}_A\right) \qquad (109)$$

We now go back to the original problem:

$$\begin{aligned} &\underset{\Omega}{\text{minimize}} \;\; \underset{b}{\max} \;\; \text{Prob}\left(\left|\hat{x}_3 - x_3\right| > VAL, y \in \Omega \mid \text{fault}\right) \\ &\text{such that Prob}\left(y \notin \Omega \mid \text{no fault}\right) = P_{fa} \end{aligned} \qquad (110)$$

After the change in variables the problem is written:

$$\underset{\Omega'}{\text{minimize}} \;\; \underset{b_V, b_{other}}{\max} \;\; \text{Prob}\left(\left|e_3^T\left(\hat{x}-x\right)\right| > VAL, \begin{bmatrix} \hat{x}_A \\ \hat{b}_V \\ \hat{b}_{other} \\ z \end{bmatrix} \in \Omega' \mid \text{fault}\right)$$

$$\text{such that Prob}\left(\begin{bmatrix} \hat{x}_A \\ \hat{b}_V \\ \hat{b}_{other} \\ z \end{bmatrix} \notin \Omega' \mid \text{no fault}\right) = P_{fa}$$

(111)

We have shown that after changing variables, the only relevant information to limit $\left|\hat{x}_3 - x_3\right|$ is included in the scalar: $e_3^T\left(\hat{x}_A - \hat{x}\right)$. As a consequence, there is no reason to limit the region **Ω'** in the other components (although intuitively obvious, the formal proof of this statement is complex and is not included here). The problem therefore becomes the search of an interval (or union of intervals) Λ such that:

$$\begin{aligned} &\underset{\Lambda}{\text{minimize}} \;\; \underset{b_V}{\max} \;\; \text{Prob}\left(\left|b_V + \sigma w_1\right| > VAL, b_V + \sigma_{ss}w_2 \in \Lambda\right) \\ &\text{such that Prob}\left(\sigma_{ss}w_2 \notin \Lambda\right) = P_{fa} \end{aligned}$$

(112)

In the above formulation we have performed the change of variables:

$$\begin{aligned} &e_3^TS\varepsilon = \sigma w_1 \\ &e_3^TSAR^{-1}A^TWP\varepsilon = \sigma_{ss}w_2 \end{aligned} \qquad (113)$$

The random variables w_1 and w_2 are independent zero mean unit Gaussian distributed. It can be shown that the optimal interval is $\Lambda = \left[-T, T\right]$ such that:

$$\text{Prob}\left(\sigma_{ss}w_2 \notin \left[-T, T\right]\right) = P_{fa} \qquad (114)$$

APPENDIX H

Protection Level Proof of Safety

Definitions

x_3 true vertical position

$\hat{x}_3^{(k)}$ estimated vertical position using subset k (position estimate tolerant to fault k). k=0 is the all in view.

$s_3^{(k)}$ coefficients projecting measurements onto the estimated position k.

$b_{nom,act}$ nominal biases (nx1 vector)

b_{nom} nominal biases bound (nx1 vector)

b_{fault} error in all in view position resulting from fault mode k

ε nominal random error

T_k threshold for solution separation for the k^{th} fault mode

$p_{ap,k}$ a priori probability of fault mode k. k=0 corresponds to the fault free mode

σ_k standard deviation of $\hat{x}_3^{(k)} - x_3$

Contribution to the integrity budget of each fault mode

Fault mode k affects the all-in-view position as follows (regardless of how many satellites are affected).

$$\hat{x}_3^{(0)} - x_3 = s_3^{(0)T}\varepsilon + s_3^{(0)T} b_{nom,act} + b_{fault}$$

$$\hat{x}_3^{(k)} - x_3 = s_3^{(k)T}\varepsilon + s_3^{(k)T} b_{nom,act} \tag{115}$$

The probability of misdetection is given by:

$$\max_{b_{fault}} P\left(\left|\hat{x}_3^{(0)} - x_3\right| > VPL, \left|\hat{x}_3^{(k)} - \hat{x}_3^{(0)}\right| < T_k\right) \tag{116}$$

To compute an upper bound of this expression, we write:

$$\begin{aligned} &P\left(\left|\hat{x}_3^{(0)} - x_3\right| > VPL, \left|\hat{x}_3^{(k)} - \hat{x}_3^{(0)}\right| < T_k\right) = \\ &P\left(\hat{x}_3^{(0)} - x_3 > VPL, \left|\hat{x}_3^{(k)} - \hat{x}_3^{(0)}\right| < T_k\right) + \\ &P\left(\hat{x}_3^{(0)} - x_3 < -VPL, \left|\hat{x}_3^{(k)} - \hat{x}_3^{(0)}\right| < T_k\right) \end{aligned} \tag{117}$$

Let us suppose that $b_{fault}>0$. (It is easy to verify that the bound will also work for $b_{fault}<0$). For each fault mode k, we have:

$$\begin{aligned} &P\left(\hat{x}_3^{(0)} - x_3 > VPL, \left|\hat{x}_3^{(k)} - \hat{x}_3^{(0)}\right| < T_k\right) \le \\ &P\left(\hat{x}_3^{(0)} - x_3 > VPL, \hat{x}_3^{(0)} - \hat{x}_3^{(k)} < T_k\right) \\ &= P\left(\hat{x}_3^{(0)} - \hat{x}_3^{(k)} + \hat{x}_3^{(k)} - x_3 > VPL, \hat{x}_3^{(0)} - \hat{x}_3^{(k)} < T_k\right) \le \\ &P\left(T_k + \hat{x}_3^{(k)} - x_3 > VPL\right) \\ &= P\left(\hat{x}_3^{(k)} - x_3 > VPL - T_k\right) \end{aligned}$$

$$\begin{aligned} &P\left(\hat{x}_3^{(0)} - x_3 < -VPL, \left|\hat{x}_3^{(k)} - \hat{x}_3^{(0)}\right| < T_k\right) = \\ &P\left(s_3^{(0)T}\varepsilon + s_3^{(0)T} b_{nom,act} + b_{fault} < -VPL, \left|\hat{x}_3^{(k)} - \hat{x}_3^{(0)}\right| < T_k\right) \le \\ &P\left(s_3^{(0)T}\varepsilon + s_3^{(0)T} b_{nom,act} < -VPL\right) \le P\left(s_3^{(0)T}\varepsilon < -VPL + \left|s_3^{(0)T} b_{nom,act}\right|\right) \\ &= P\left(s_3^{(0)T}\varepsilon > VPL - \left|s_3^{(0)}\right|^T b_{nom}\right) \end{aligned} \tag{118}$$

In the above equation, the notation $\left|s_3^{(0)}\right|^T$ means that we take the component-wise absolute value of each coordinate (to avoid writing a sum). To summarize we have:

$$\begin{aligned} &\max_{b_{fault}} P\left(\left|\hat{x}_3^{(0)} - x_3\right| > VPL, \left|\hat{x}_3^{(k)} - \hat{x}_3^{(0)}\right| < T_k\right) \le \\ &P\left(\hat{x}_3^{(k)} - x_3 > VPL - T_k\right) + P\left(s_3^{(0)T}\varepsilon > VPL - \left|s_3^{(0)}\right|^T b_{nom}\right) \end{aligned} \tag{119}$$

We also have:

$$\begin{aligned} &P\left(\hat{x}_3^{(k)} - x_3 > VPL - T_k\right) = P\left(s_3^{(k)T}\varepsilon + s_3^{(k)T} b_{nom} > VPL - T_k\right) \\ &= P\left(s_3^{(k)T}\varepsilon > VPL - T_k - s_3^{(k)T} b_{nom}\right) \le P\left(s_3^{(k)T}\varepsilon > VPL - T_k - \left|s_3^{(k)}\right|^T b_{nom}\right) \\ &= Q\left(\frac{VPL - T_k - \left|s_3^{(k)}\right|^T b_{nom}}{\sqrt{s_3^{(k)T}\operatorname{cov}(\varepsilon) s_3^{(k)}}}\right) = Q\left(\frac{VPL - T_k - \left|s_3^{(k)}\right|^T b_{nom}}{\sigma_k}\right) \end{aligned} \tag{120}$$

The second term is actually only a particular case of the above equation:

$$P\left(s_3^{(0)T}\varepsilon > VPL - \left|s_3^{(0)}\right|^T b_{nom}\right) \le Q\left(\frac{VPL - \left|s_3^{(0)}\right|^T b_{nom}}{\sigma_0}\right) \tag{121}$$

The probability of HMI is therefore given by:

$$\sum_{k=0}^{N_{faults}} p_{ap,k}\left(Q\left(\frac{VPL-T_k-\left|s_3^{(k)}\right|^T b_{nom}}{\sigma_k}\right)+Q\left(\frac{VPL-\left|s_3^{(0)}\right|^T b_{nom}}{\sigma_0}\right)\right) \tag{122}$$

The second term can be re-grouped as follows:

$$\begin{aligned}
&\sum_{k=0}^{N_{faults}} p_{ap,k}\left(Q\left(\frac{VPL-T_k-\left|s_3^{(k)}\right|^T b_{nom}}{\sigma_k}\right)+Q\left(\frac{VPL_k-\left|s_3^{(0)}\right|^T b_{nom}}{\sigma_0}\right)\right)\\
&=2p_{ap,0}Q\left(\frac{VPL-\left|s_3^{(0)}\right|^T b_{nom}}{\sigma_0}\right)+\left(\sum_{k=1}^{N_{faults}} p_{ap,k}\right)Q\left(\frac{VPL-\left|s_3^{(0)}\right|^T b_{nom}}{\sigma_0}\right)+\\
&\sum_{k=1}^{N_{faults}} p_{ap,k}Q\left(\frac{VPL-T_k-\left|s_3^{(k)}\right|^T b_{nom}}{\sigma_k}\right)\\
&=2\left(p_{ap,0}+\frac{1}{2}\sum_{k=1}^{N_{faults}} p_{ap,k}\right)Q\left(\frac{VPL-\left|s_3^{(0)}\right|^T b_{nom}}{\sigma_0}\right)+\\
&\sum_{k=1}^{N_{faults}} p_{ap,k}Q\left(\frac{VPL-T_k-\left|s_3^{(k)}\right|^T b_{nom}}{\sigma_k}\right)
\end{aligned} \tag{123}$$

We have:

$$p_{ap,0}+\sum_{k=1}^{N_{faults}} p_{ap,k}=1 \text{ so } p_{ap,0}+\frac{1}{2}\sum_{k=1}^{N_{faults}} p_{ap,k}\leq 1 \tag{124}$$

This means that the formulation of SS ARAIM with one sided cdf for all faults except the nominal strictly meets the integrity requirement, as long as the probability of the fault free is taken to be larger than:

$$p_{ap,0}+\frac{1}{2}\sum_{k=1}^{N_{faults}} p_{ap,k} \tag{125}$$

instead of $p_{ap,0}$. In the proposed algorithm, this condition is met because we use a prior of 1 for the fault free case.

APPENDIX I

Rank One Update Formulas

We show formulas that link the estimation coefficients S from a set of satellites to a set of satellites minus one satellite. These formulas can greatly speed up the user algorithm, because it is not necessary to invert a 5 by 5 matrix for each subset.

We consider a diagonal weighting matrix:

$$W = diag\left(\begin{bmatrix} w_1 & \cdots & w_n \end{bmatrix}\right) \tag{126}$$

And an observation matrix:

$$G=\begin{bmatrix} g_1^T \\ \vdots \\ g_n^T \end{bmatrix} \tag{127}$$

In the following equations, the index with the hat indicates that we have removed that index from the matrix.

Covariance matrix update:

$$\left(G_{\hat{i}}^T W_{\hat{i}} G_{\hat{i}}\right)^{-1}=\left(G^T W G\right)^{-1}+\frac{\left(G^T W G\right)^{-1}\left(g_i w_i g_i^T\right)\left(G^T W G\right)^{-1}}{1-g_i^T w_i \left(G^T W G\right)^{-1} g_i} \tag{128}$$

Chi-square statistic update:

$$\begin{aligned}
&y_{\hat{i}}^T W_{\hat{i}} y_{\hat{i}}-\left(G_{\hat{i}}^T W_{\hat{i}} y_{\hat{i}}\right)^T\left(G_{\hat{i}}^T W_{\hat{i}} G_{\hat{i}}\right)^{-1} G_{\hat{i}}^T W_{\hat{i}} y_{\hat{i}} =\\
&y^T W y - y^T W G\left(G^T W G\right)^{-1} G^T W y\\
&-\frac{w_i}{1-g_i^T w_i\left(G^T W G\right)^{-1} g_i}\left(y_i-g_i^T\left(G^T W G\right)^{-1} G^T W y\right)^2
\end{aligned} \tag{129}$$

Or:

$$\chi_{\hat{i}}^2=\chi^2-\frac{w_i}{1-g_i^T w_i\left(G^T W G\right)^{-1} g_i}\left(y_i-g_i^T\left(G^T W G\right)^{-1} G^T W y\right)^2 \tag{130}$$

Position solution update

Here we specify the difference between the position solutions whether we use the full set of measurements or the subset with one satellite out:

$$\left(G^TWG\right)^{-1}G^TWy-\left(G_{\hat{i}}^TW_{\hat{i}}G_{\hat{i}}\right)^{-1}G_{\hat{i}}^TW_{\hat{i}}y_{\hat{i}} = \frac{\left(G^TWG\right)^{-1}g_iw_i}{1-g_i^Tw_i\left(G^TWG\right)^{-1}g_i}\left(y_i-g_i^T\left(G^TWG\right)^{-1}G^TWy\right) \quad (131)$$

Or:

$$\hat{x}-\hat{x}_{\hat{i}} = \frac{\left(G^TWG\right)^{-1}g_iw_i}{1-g_i^Tw_i\left(G^TWG\right)^{-1}g_i}\left(y_i-g_i^T\left(G^TWG\right)^{-1}G^TWy\right)$$

(132)

APPENDIX J

Numerical example

We consider the geometry defined by G:

```
G = [0.0225   0.9951  -0.0966  1  0;
     0.6750  -0.6900  -0.2612  1  0;
     0.0723  -0.6601  -0.7477  1  0;
    -0.9398   0.2553  -0.2269  1  0;
    -0.5907  -0.7539  -0.2877  1  0;
    -0.3236  -0.0354  -0.9455  0  1;
    -0.6748   0.4356  -0.5957  0  1;
     0.0938  -0.7004  -0.7075  0  1;
     0.5571   0.3088  -0.7709  0  1;
     0.6622   0.6958  -0.2780  0  1];
```

(133)

We assume that for all satellites:

$$\sigma_{URA,i}=.75 \text{ m} \qquad \sigma_{URE,i}=.50 \text{ m} \qquad P_{sat,i}=10^{-4}$$
$$b_{nom,i} = .5 \text{ m}$$

(134)

For the two constellations we assume:

$$P_{const,j}=10^{-4}$$

(135)

Following the steps outlined in the paper and using the preliminary values introduced in the list of constants we have:

$$C_{\text{int}} = diag\begin{pmatrix} [3.8865 & 1.4377 & 0.8604 & 1.6383 & 1.3229 \\ 0.8434 & 0.8963 & 0.8669 & 0.8573 & 1.3616] \end{pmatrix}$$
$$C_{acc} = diag\begin{pmatrix} [3.5740 & 1.1252 & 0.5479 & 1.3258 & 1.0104 \\ 0.5309 & 0.5838 & 0.5544 & 0.5448 & 1.0491] \end{pmatrix}$$

$$N_{sat,\max} = 2$$
$$N_{const,\max} = 1$$

(136)

That is, subset fault modes include all *n-1* and *n-2* subsets, as well as the two constellation fault modes. For the two constellation fault modes we have:

$$\sigma_3^{(k)} = 2.5760 \text{ m} \qquad \sigma_3^{(k')} = 2.5577 \text{ m}$$
$$\sigma_{ss,3}^{(k)} = 1.5307 \text{ m} \qquad \sigma_{ss,3}^{(k')} = 1.5292 \text{ m}$$
$$b_3^{(k)} = 2.8935 \text{ m} \qquad b_3^{(k')} = 2.0875 \text{ m}$$

(137)

(We do not write the standard deviations for all the other subsets). We have:

$$K_{fa,3} = Q^{-1}\left(\frac{P_{FA\_VERT}}{2N_{fault\ \text{modes}}}\right) = Q^{-1}\left(\frac{3.9\times10^{-6}}{2\times57}\right) = 5.3953$$

(138)

The solution to Equation (24) is:

$$VPL = 19.7\ m$$

The HPL is given by Equation (26) and is:

$$HPL = 14.9\ m$$

The EMT is given by Equation (32) and is:

$$EMT = 11.8\ m$$

The standard deviation of the all-in-view given by Equation (27) is:

$$\sigma_{v,acc} = 1.47 \text{ m}$$

APPENDIX K

We provide elements for the proof of Equation (49). The worst case integrity contribution is given by:

$$\max_{b_{fault}} P\left(\hat{x}_3^{(0)} - x_3 > VPL, \hat{x}_3^{(0)} - \hat{x}_3^{(k)} < T_k\right)$$
$$= \max_{b_{fault}} P\begin{pmatrix} s_3^{(0)T}\varepsilon + s_3^{(0)T}b_{nom} + b_{fault} > VPL, \\ \left(s_3^{(0)} - s_3^{(k)}\right)\varepsilon + \left(s_3^{(0)} - s_3^{(k)}\right)b_{nom} + b_{fault} < T_k \end{pmatrix} \quad (139)$$

As we are maximizing over b_{fault}, we can change the variables as follows:

$$b_{fault} + s_3^{(0)T}b_{nom} \rightarrow b_{fault} \quad (140)$$

Under the integrity error model we have:

$$s_3^{(0)T}\varepsilon \sim N\left(0,\sigma_3^{(0)}\right)$$
$$s_3^{(k)T}\varepsilon \sim N\left(0,\sqrt{\sigma_3^{(k)2}-\sigma_3^{(0)2}}\right) \quad (141)$$

In addition, these two random variables are independent. As a consequence, we have:

$$\max_{b_{fault}} P\left(\hat{x}_3^{(0)}-x_3 > VPL, \hat{x}_3^{(0)}-\hat{x}_3^{(k)} < T_k\right)$$
$$= \max_{b_{fault}} P\left(\begin{array}{l}\dfrac{s_3^{(0)T}\varepsilon}{\sigma_3^{(0)}} > \dfrac{VPL-b_{fault}}{\sigma_3^{(0)}},\\ \dfrac{\left(s_3^{(0)}-s_3^{(k)}\right)\varepsilon}{\sqrt{\sigma_3^{(k)2}-\sigma_3^{(0)2}}} < \dfrac{T_k+s_3^{(k)}b_{nom}-b_{fault}}{\sqrt{\sigma_3^{(k)2}-\sigma_3^{(0)2}}}\end{array}\right) \quad (142)$$
$$= \max_{b_{fault}} Q\left(\frac{VPL-b_{fault}}{\sigma_3^{(0)}}\right) Q\left(-\frac{T_k+s_3^{(k)}b_{nom}-b_{fault}}{\sqrt{\sigma_3^{(k)2}-\sigma_3^{(0)2}}}\right)$$

Equation (49) can be obtained from (142) using the appropriate change of variables and noticing that $s_3^{(k)}b_{nom} \le b_3^{(k)}$.

REFERENCES

[1] RTCA/DO-208, "Minimum Operational Performance Standards for Airborne Supplemental Navigation Equipment Using Global Positioning System (GPS)," RTCA/DO-208, July 1991, prepared by RTCA Special Committee 159

[2] "Airborne Supplemental Navigation Equipment Using the Global Positioning System (GPS)," Technical Standard Order (TSO) C-129, 10 December 1992, U.S. Federal Aviation Administration, Washington, D.C.

[3] Murphy, T., Harris, M., "RAIM Performance in the Post SA Era," *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, Savannah, GA, September 2008, pp. 139-150.

[4] Dufresne, C., Hansen, A., O'Neill, K., Parmet, J., Volchansky, L., "Global Positioning System (GPS) Receiver Autonomous Integrity Monitoring (RAIM) Web Service to Support Area Navigation (RNAV) Flight Planning," *Proceedings of the 2008 National Technical Meeting of The Institute of Navigation*, San Diego, CA, January 2008, pp. 402-406.

[5] www.raimprediction.net

[6] Phase II of the GNSS Evolutionary Architecture Study, February 2010 http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/library/documents/media/GEASPhaseII_Final.pdf

[7] Hegarty, C., Chatre, E. "Evolution of the Global Navigation Satellite System (GNSS)," *Proc. IEEE*, vol. 96, pp. 1902 – 1917

[8] DeCleene, B., "Performance Requirements for LPV Approaches to Minima as Low as 200 ft above Runway Threshold," *International Civil Aviation Organization Navigation Systems Panel (NSP), Technical Working Group (WG1) Meeting*, Brussels, Belgium, May 8 to 19, 2006

[9] Blanch, J., Walter, T., Enge, P., Wallner, S., Fernandez, F., Dellago, R., Ioannides, R., Pervan, B., Hernandez, I., Belabbas, B., Spletter, A., and Rippl, M., "Critical Elements for a Multi-Constellation Advanced RAIM", *NAVIGATION*, Vol. 60, No. 1, Spring 2013, pp. 53-69.

[10] Blanch, J., Walter, T., Enge, P. "Framework for analyzing ARAIM architectures," *Proceedings of the Institute of Navigation GNSS-12*, Nashville, September 2012.

[11] Blanch, J., Ene, A., Walter, T., Enge, P., "An Optimized Multiple Hypothesis RAIM Algorithm for Vertical Guidance," *Proceedings of the 20th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2007)*, Fort Worth, TX, September 2007, pp. 2924-2933.

[12] Blanch, J., Walter, T., Enge, P. "RAIM with Optimal Integrity and Continuity Allocations Under Multiple failures," *IEEE Transactions on Aerospace and Electronic Systems* Vol. 46, No. 3, July 2010.

[13] Ene, A., "Utilization of Modernized Global Navigation Satellite Systems for Aircraft-Based Navigation Integrity," Doctoral Research Dissertation, VDM VerlagDr. Müller, June 2009.

[14] ICAO, Annex 10, Aeronautical Telecommunications, Volume 1 (Radio Navigation Aids), Amendment 84, published 20 July 2009, effective 19 November 2009. GNSS standards and recommended practices (SARPs) are contained in Section 3.7 and subsections, Appendix B, and Attachment D.

[15] WAAS Minimum Operational Performance Specification (MOPS), RTCA document DO-229D

[16] Blanch, J. " Potential ARAIM Improvements", Briefing presented at the EU-US Cooperative WG-C ARAIM Subgroup Meeting in Munich, January 2012.

[17] Amarillo, F. "MHSS RAIM with Q transformation" Briefing presented at the EU-US Cooperative WG-C ARAIM Subgroup Meeting in Munich, January 2012.

[18] Lee, Y., "RAIM Using Two Constellations to Provide Integrity for LPV-200 In the Presence of an EOP Fault," Briefing Presented at the EU-US Cooperative WG-C ARAIM Subgroup Meeting, Stanford University, California, June 20, 2011

[19] Lee, Y., "New Advanced ARAIM with Improved Availability for Detecting Constellation-wide Faults, Using two Independent Constellations," *Proceedings of the 2012 International Technical Meeting of The Institute of Navigation*, Newport Beach, CA, January 2012, pp. 1708-.

[20] Blanch, J., "MHSS ARAIM Algorithm and Constrained Constellation Faults," Briefing Presented at the EU-US Cooperative WG-C ARAIM Subgroup Meeting, Portland, September 2011.

[21] Lee, Y., "New Advanced ARAIM with Improved Availability for Detecting Constellation-wide Faults, Using two Independent Constellations," *Proceedings of the 2012 International Technical Meeting of The Institute of Navigation*, Newport Beach, CA, January 2012, pp. 1708-.

[22] B. Pervan, S. Langel, J. Meno, M. Joerger, and F.-C. Chan, "Maturation of EOP Threat Model," Briefing presented at the WGC ARAIM SG meeting in Munich, January 18, 2012

[23] Global Positioning System Standard Position Service Performance Standard, , 4th Edition, September 2008

[24] B. Pervan, "Maturation of EOP Threat Model," Briefing presented at the WGC ARAIM SG teleconference, March 20, 2012

[25] Garrison and Eichel, "An Extended Propagation Ephemeris for GNSS," *NAVIGATION*, Vol. 53, No. 3, Fall 2006.

[26] Hwang, P., Brown, R. G., "RAIM FDE Revisited: A New Breakthrough In Availability Performance With NIORAIM (Novel Integrity-Optimized RAIM)," *Proceedings of the 2005 National Technical Meeting of The Institute of Navigation*, San Diego, CA, January 2005, pp. 654-665.

[27] Lee, Y., "Two New RAIM Methods Based on the Optimally Weighted Average Solution (OWAS) Concept", *NAVIGATION*, Vol. 54, No. 4, Winter 2007, pp. 333-345.

[28] Blanch, J., Walter, T., Enge, P., "Optimal Positioning for Advanced RAIM," *Proceedings of the 2012 International Technical Meeting of The Institute of Navigation*, Newport Beach, CA, January 2012, pp. 1624-0.

[29] RTCA/DO-208, "Minimum Operational Performance Standards for Airborne Supplemental Navigation Equipment Using Global Positioning System (GPS)," RTCA/DO-208, July 1991, prepared by RTCA Special Committee 159

[30] McGraw et. al, "Development of the LAAS Accuracy Models," *Proceedings of the ION GPS 2000*, Salt Lake City, UT

[31] "Airborne Supplemental Navigation Equipment Using the Global Positioning System (GPS)," Technical Standard Order (TSO) C-129, 10 December 1992, U.S. Federal Aviation Administration, Washington, D.C.

[32] Heng, L., Gao, G.X., Walter, T., Enge, P., "GPS Signal-in-Space Anomalies in the Last Decade: Data Mining of 400,000,000 GPS Navigation Messages," *Proceedings of the 23rd International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2010)*, Portland, OR, September 2010, pp. 3115-3122.