

Integrity Risk and Continuity Risk for Fault Detection and Exclusion Using Solution Separation ARAIM

Mathieu Joerger, Stefan Stevanovic, Fang-Cheng Chan, Steven Langel,
and Boris Pervan, *Illinois Institute of Technology*

BIOGRAPHIES

Dr. Mathieu Joerger obtained a Master in Mechatronics from the National Institute of Applied Sciences in Strasbourg, France, in 2002, and a M.S. and a Ph.D. in Mechanical and Aerospace Engineering from the Illinois Institute of Technology (IIT), in 2002 and 2009 respectively. He is the 2009 recipient of the Institute of Navigation (ION) Bradford Parkinson award, which honors outstanding graduate students in the field of GNSS. He is currently a research assistant professor at IIT, working on multi-sensor integration, on sequential fault-detection for multi-constellation navigation systems, and on relative and differential receiver autonomous integrity monitoring (RAIM) for shipboard landing of military aircraft.

Stefan Stevanovic is a PhD candidate at IIT whose research focuses on RAIM algorithms for carrier phase differential GPS applications including the shipboard landing of aircraft. Stefan received his B.S. in mechanical engineering and M.S. in mechanical and aerospace engineering from IIT.

Dr. Fang-Cheng Chan is a Senior Research Associate at Navigation Laboratory in the Department of Mechanical and Aerospace Engineering at IIT in Chicago. He received his Ph.D in mechanical and aerospace engineering from IIT, Chicago, in 2008. He is currently working on GPS receiver integrity for Local Area Augmentation System (LAAS) ground receivers, researching for GPS receiver interference detection and mitigation to prevent unintentional jamming using both baseband and antenna array techniques, and developing navigation and fault detection algorithms for Technical Subgroup of EU/US Working Group C (WGC) with focus on RAIM. Dr. Chan is a member of American Institute of Aeronautics and Astronautics, and a member of ION.

Steven Langel is a PhD candidate at IIT whose work focuses on the design of high accuracy, high integrity navigation algorithms for aerospace applications.

Specific research interests include carrier phase differential GPS navigation with cycle resolution, Kalman filtering with stochastic modeling uncertainty and the design of GPS / INS integration algorithms. Steven received his B.S. degree in mechanical and aerospace engineering from IIT.

Dr. Boris Pervan is a Professor of Mechanical and Aerospace Engineering at IIT, where he conducts research on advanced navigation systems. Prior to joining the faculty at IIT, he was a spacecraft mission analyst at Hughes Aircraft Company (now Boeing) and a postdoctoral research associate at Stanford University. Prof. Pervan received his B.S. from the University of Notre Dame, M.S. from the California Institute of Technology, and Ph.D. from Stanford University. He is an Associate Fellow of the AIAA, a Fellow of the Institute of Navigation (ION), and Editor-in-Chief of the ION journal *NAVIGATION*. He was the recipient of the IIT Sigma Xi Excellence in University Research Award (2011, 2002), Ralph Barnett Mechanical and Aerospace Dept. Outstanding Teaching Award (2009, 2002), Mechanical and Aerospace Dept. Excellence in Research Award (2007), University Excellence in Teaching Award (2005), IEEE Aerospace and Electronic Systems Society M. Barry Carlton Award (1999), RTCA William E. Jackson Award (1996), Guggenheim Fellowship (Caltech 1987), and Albert J. Zahm Prize in Aeronautics (Notre Dame 1986).

ABSTRACT

The increased number of redundant ranging signals in future multi-constellation GNSS will improve RAIM-based integrity monitoring performance, but will also increase the probability of satellite faults, thereby increasing the continuity risk. In response, in this paper, a solution separation (SS) approach to fault detection and exclusion (FDE) is developed.

The first part of the paper proves that for single-measurement faults, SS detection test statistics are projections of the parity vector on failure mode lines. It follows that the SS detection boundary can be represented as a polytope in parity space. To further analyze this result, we design a method that provides a piecewise linear detection boundary, which minimizes the integrity risk while limiting the probability of false alarms. This optimal detection region varies with navigation system parameters, but for realistic, practical requirements, the optimal detection region approaches the SS polytope-shaped boundary.

The second part of the paper introduces complete integrity risk and continuity risk equations for SS fault detection *and exclusion*. Probability bounds are developed, which express the reduction of continuity risk using exclusion at the cost of increased integrity risk. The integrity risk bound (also given in the form of protection levels) is designed to enable risk evaluation in practical applications where computation resources are limited. In parallel, a continuity risk bound is derived, which provides the means to determine detection and exclusion thresholds that satisfy the continuity risk requirement. Parity space representations reveal the shape of the SS exclusion zones, and reaffirm the convenience of using normally-distributed SS test statistics for risk evaluation, especially in high-dimensional parity space. Finally, the SS FDE integrity and continuity risk bounds are implemented to establish worldwide availability maps for an example aircraft approach application using Advanced RAIM (ARAIM) based on GPS and Galileo measurements.

I. INTRODUCTION

This paper describes the derivation, analysis and evaluation of fault detection and exclusion (FDE) algorithms based on solution separation (SS) receiver autonomous integrity monitoring (RAIM). First, a parity space representation of the SS FDE method is introduced. Then, complete integrity risk and continuity risk equations, which are currently lacking in the literature, are developed for SS FDE.

Global navigation satellite system (GNSS) measurements are vulnerable to rare-event faults including satellite failures, which represent major integrity threats in safety-critical applications. In response, fault-detection algorithms such as RAIM can be implemented. RAIM exploits redundant ranging signals to achieve self-contained fault detection at the user receiver.

With the modernization of GPS, the full deployment of GLONASS, and the emergence of Galileo and Beidou, an increased number of redundant measurements becomes available, which has recently drawn a renewed interest in

RAIM. In particular, RAIM can help alleviate requirements on ground monitors. For example, researchers in the European Union and in the United States are investigating Advanced RAIM (ARAIM) for worldwide vertical guidance of aircraft [1], [2].

Two conflicting aspects of RAIM-based fault-detection will arise from the addition of new redundant ranging signals in future multi-constellation GNSS. On the one hand, the integrity monitoring performance using ARAIM will improve [3]. On the other hand, the heightened likelihood of satellite faults will cause more occurrences of mission interruptions due to faults being detected, thereby increasing the continuity risk.

In response, fault exclusion procedures have been designed [4], [5], [6], which, unfortunately, do not provide the means to reliably predict the integrity and continuity risks [7], [8]. Integrity risk evaluation is challenging because it involves quantifying the impact on state estimate errors of undetected faults and of wrong exclusions. Without integrity and continuity risk equations for detection and exclusion, it remains unclear whether the overall navigation performance (including both integrity and continuity) will keep improving as the number of satellite signals increases. Therefore, this work aims at providing integrity and continuity risk equations for fault detection *and exclusion*.

This paper starts by addressing RAIM-based fault detection only. In a previous publication [9], we pointed out differences between two of the most widely-implemented detection methods: SS and chi-squared residual (χ^2) RAIM. It was shown that the SS detection performance was higher than χ^2 because SS test statistics are tailored to the fault hypotheses, and to the state of interest.

We pursue this analysis in Sections II and III of this paper by providing a parity space representation of the SS method. The parity vector is the simplest, most fundamental expression of the detection capability. For single-satellite faults, the SS test statistics are proved to be projections of the parity vector on fault mode lines (which are defined in the paper). It follows that the SS detection boundary can be represented in parity space as a polytope.

Section IV aims at determining the shape of the ‘optimal’ detection boundary, which minimizes the integrity risk while satisfying a false-alarm requirement. The proposed method approximates the optimal detection region using a piecewise linear boundary, whose segments are determined by solving a constrained minimization problem. Section IV shows that for practical, realistic requirements, the optimal detection region matches the SS

polytope-shaped boundary. This is why a SS approach to exclusion is considered.

Section V presents a complete derivation of the integrity and continuity risk equations for SS RAIM FDE. These equations quantify the price paid in terms of integrity risk for reducing the continuity risk using exclusion. First, a probability bound is established, which enables integrity risk evaluation using protection levels in practical implementations where computation resources are limited. Second, a continuity risk bound is developed, which provides the means to determine detection and exclusion thresholds while ensuring that the overall continuity risk requirement is satisfied. Third, a parity space representation of the SS exclusion zones is given, which underlines the practical benefit of using normally-distributed SS test statistics for risk evaluation.

Finally, in Section VI, a performance analysis is carried out to assess worldwide availability of SS ARAIM FDE for an example aircraft approach navigation application. Availability maps illustrate that the methods derived in this paper go beyond previous preliminary analyses [3], as they enable the evaluation not only of the integrity risk and probability of false alarms, but also of the overall continuity risk.

II. INTEGRITY RISK EVALUATION FOR RAIM FAULT DETECTION

This section outlines the integrity risk evaluation method for detection only, which involves quantifying the impact of undetected faults on the estimation error. The integrity risk is first defined in Section II-A, followed by a model of the measurements (II-B), which are then used to determine the estimation error (II-C) and the detection test statistics given in Section III.

A. Integrity Risk Definition for Detection Only

In RAIM-based fault detection, the integrity risk or probability of hazardous misleading information (HMI) is defined as the following joint probability:

$$P_{HMI} \equiv P(\varepsilon_0 > \ell, |q| < T) \quad (1)$$

where

- ε_0 is the estimate error for the state of interest (discussed in Section II.C)
- ℓ is a specified alert limit that defines hazardous situations
- q is the detection test statistic (described in Section III)
- T is the detection threshold

In addition, considering a set of $n_H + 1$ mutually exclusive, exhaustive hypotheses H_i , the law of total probability can be used to express equation (1) as:

$$P_{HMI} = \sum_{i=0}^{n_H} P(\varepsilon_0 > \ell, |q| < T | H_i) P_{H_i} \quad (2)$$

where

P_{H_i} is the prior probability of H_i occurrence

H_0 is the fault-free (FF) hypothesis

H_i for $i=1, \dots, n_H$ are the fault hypotheses corresponding to faults on subset measurement ‘ i ’

In general, fault hypotheses H_i can include faults simultaneously affecting multiple measurements. These cases are included in Section V. However, in Sections II to IV, we limit the analysis to single-measurement faults.

Under the FF hypothesis H_0 , the detection threshold T can be set in accordance with a continuity risk requirement allocation C_{REQ0} to limit the probability of false alarms. T can be defined as:

$$P(q \geq T | H_0) P_{H_0} \leq C_{REQ0} \quad (3)$$

B. Measurement Equation

The estimate error ε_0 and test statistic q in equation 2 are evaluated using a measurement model. Let n and m respectively be the numbers of measurements and of states. The $n \times 1$ measurement vector \mathbf{z}_* is assumed normally distributed with mean vector $\boldsymbol{\mu}_{\mathbf{z}_*}$ and covariance matrix \mathbf{V}_* . We use the notation:

$$\mathbf{z}_* \sim \mathbf{N}(\boldsymbol{\mu}_{\mathbf{z}_*}, \mathbf{V}_*) \quad (4)$$

Matrix \mathbf{V}_* is assumed to be diagonal (for reasons explained below), with strictly positive diagonal elements. Vector \mathbf{z}_* in equation (4) can be pre-multiplied by $\mathbf{V}_*^{-1/2}$ to obtain the measurement equation:

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{v} + \mathbf{f} \quad (5)$$

where

- $\mathbf{z} = \mathbf{V}_*^{-1/2} \mathbf{z}_*$ is the ‘normalized’ measurement vector
- \mathbf{H} is the $n \times m$ normalized observation matrix,
- \mathbf{x} is the $m \times 1$ state vector,

- \mathbf{v} is the $n \times 1$ normalized measurement noise vector composed of independent and identically distributed (i.i.d.) random variables
- \mathbf{f} is the $n \times 1$ normalized fault vector.

The measurement vector $\mathbf{z} \sim \mathbf{N}(\mathbf{0}, \mathbf{I})$, where $\mathbf{0}$ is a matrix of zeros of appropriate dimension ($n \times 1$ in this case) and \mathbf{I} is the identity matrix of appropriate dimension ($n \times n$ in this case).

To address the diagonal \mathbf{V}_* assumption, it is worth reminding that RAIM-type detection methods are based on measurement redundancy and are therefore only effective against faults affecting a maximum number of $n - m$ measurements. Matrix \mathbf{V}_* was earlier assumed to be diagonal to ensure that single elements of the original fault vector \mathbf{f}_* would not impact multiple elements of \mathbf{f} through to the pre-multiplication by $\mathbf{V}_*^{-1/2}$ (in equations (4) to (5), we assumed $\mathbf{f} = \mathbf{V}_*^{-1/2} \mathbf{f}_*$).

C. Example Estimator: Least Squares

In this paper, we consider a least-squares estimator, but the derivations in Section V do not require this assumption. The state estimate error vector is defined as:

$$\boldsymbol{\varepsilon}_0 \equiv \mathbf{S}_0(\mathbf{v} + \mathbf{f}) \quad \text{and} \quad \boldsymbol{\varepsilon}_0 \sim \mathbf{N}(\mathbf{S}_0 \mathbf{f}, \mathbf{P}_0) \quad (6)$$

$$\text{where} \quad \mathbf{P}_0 = (\mathbf{H}^T \mathbf{H})^{-1} \quad \text{and} \quad \mathbf{S}_0 = \mathbf{P} \mathbf{H}^T \quad (7)$$

If the focus of the integrity analysis is on a single state of interest (e.g., on the vertical position coordinate for aircraft precision approach navigation), then a single row of the least-squares estimation matrix \mathbf{S}_0 is needed, and is noted:

$$\mathbf{s}_0^T = \boldsymbol{\alpha}^T \mathbf{S}_0 \quad (8)$$

$$\text{where} \quad \boldsymbol{\alpha}^T = [\mathbf{0} \quad 1 \quad \mathbf{0}] \quad (9)$$

The scalar estimate error ε_0 in the integrity risk equation (2) can be expressed as:

$$\varepsilon_0 \equiv \boldsymbol{\alpha}^T \boldsymbol{\varepsilon}_0 = \mathbf{s}_0^T \mathbf{z} \quad (10)$$

$$\varepsilon_0 \sim \mathbf{N}(\mathbf{s}_0^T \mathbf{f}, \sigma_0^2 \equiv \boldsymbol{\alpha}^T \mathbf{P}_0 \boldsymbol{\alpha}) \quad (11)$$

Without loss of generality, it is assumed that under hypothesis H_i faults are simultaneously affecting the first n_i measurements of \mathbf{z} . In anticipation of the

solution-separation description, the measurement equation (5) can be partitioned to distinguish the subset of faulty measurements (first n_i measurements) from fault-free measurements:

$$\begin{bmatrix} \mathbf{A}_i^T \mathbf{z} \\ \mathbf{B}_i^T \mathbf{z} \end{bmatrix} = \begin{bmatrix} \mathbf{A}_i^T \mathbf{H} \\ \mathbf{B}_i^T \mathbf{H} \end{bmatrix} \mathbf{x} + \begin{bmatrix} \mathbf{A}_i^T \mathbf{v} \\ \mathbf{B}_i^T \mathbf{v} \end{bmatrix} + \begin{bmatrix} \mathbf{A}_i^T \mathbf{f} \\ \mathbf{0} \end{bmatrix} \quad (12)$$

with

$$\mathbf{A}_i \equiv \begin{bmatrix} \mathbf{I}_{n_i} \\ \mathbf{0} \end{bmatrix} \quad \text{and} \quad \mathbf{B}_i \equiv \begin{bmatrix} \mathbf{0} \\ \mathbf{I}_{n-n_i} \end{bmatrix} \quad (13)$$

where \mathbf{I}_{n_i} is the $n_i \times n_i$ identity matrix.

We distinguish the full-set solution ε_0 derived above using all n measurements, from the subset solution ε_i derived using the *fault-free* measurement subset:

$$\varepsilon_i \equiv \boldsymbol{\alpha}^T \mathbf{S}_i \mathbf{z} = \mathbf{s}_i^T \mathbf{z} \quad (14)$$

$$\varepsilon_i \sim \mathbf{N}(\mathbf{0}, \sigma_i^2 \equiv \boldsymbol{\alpha}^T \mathbf{P}_i \boldsymbol{\alpha}) \quad (15)$$

$$\text{where} \quad \mathbf{S}_i = \mathbf{P}_i \mathbf{H}^T \mathbf{B}_i \mathbf{B}_i^T \mathbf{V}^{-1} \mathbf{B}_i \quad (16)$$

$$\mathbf{P}_i = (\mathbf{H}^T \mathbf{B}_i \mathbf{B}_i^T \mathbf{V}^{-1} \mathbf{B}_i \mathbf{B}_i^T \mathbf{H})^{-1} \quad (17)$$

Finally, using a least-squares estimator and a detection test statistic q derived from the parity vector (as explained in Section III), the estimate error ε_0 and q are statistically independent, so that the joint probability in equation (2) can be expressed as:

$$P_{HMI} = \sum_{i=0}^{n_H} P(\left| \varepsilon_0 \right| > \ell \mid H_i) P(q < T \mid H_i) P_{H_i} \quad (18)$$

Sections III and IV focus on the probability of no detection $P(q < T \mid H_i)$. In Section III, we analyze two of the most widely-implemented detection methods in RAIM: the chi-squared residual (χ^2) and the solution separations (SS).

III. PARITY SPACE REPRESENTATION OF TWO DETECTION METHODS

Sections III-A and III-B provide analytical expressions of the χ^2 and SS test statistics in terms of the parity vector, Section III-C displays representations of these test statistics in parity space for single-measurement faults.

Both the χ^2 and SS test statistics are derived from the $(n-m) \times 1$ parity vector \mathbf{p} , which lays in the $(n-m)$ -dimensional parity space or left null space of \mathbf{H}^T , and can be expressed as [10]:

$$\mathbf{p} \equiv \mathbf{Q}\mathbf{z} \quad (19)$$

where the $(n-m) \times n$ parity matrix \mathbf{Q} is defined as:

$$\mathbf{Q}\mathbf{Q}^T = \mathbf{I} \quad \text{and} \quad \mathbf{Q}\mathbf{H} = \mathbf{0} \quad (20)$$

Substituting equation (5) into (19), and using the second equation in (20), \mathbf{p} is rewritten as:

$$\mathbf{p} = \mathbf{Q}(\mathbf{v} + \mathbf{f}) \quad (21)$$

Equation (21) shows that \mathbf{p} is not a function of \mathbf{x} , and is a scaled and noisy observation of the fault vector \mathbf{f} . This is why \mathbf{p} is used as a basis for fault detection.

It is also worth noticing that the measurement vector can be broken down into two orthogonal components respectively laying in the column space of \mathbf{H} and in the null space of \mathbf{H}^T [10], and expressed as:

$$\mathbf{z} = \mathbf{H}\mathbf{S}\mathbf{z} + \mathbf{Q}^T\mathbf{Q}\mathbf{z} \quad (22)$$

A. Chi-Squared Residual

The χ^2 residual test statistic is defined as the norm squared of \mathbf{p} :

$$q^2 \equiv \mathbf{p}^T \mathbf{p} \quad (23)$$

Adding and subtracting $\mathbf{H}\mathbf{S}\mathbf{z}$ to \mathbf{z} , the measurement vector can be rewritten as:

$$\mathbf{z} = \mathbf{H}\mathbf{S}\mathbf{z} + (\mathbf{I} - \mathbf{H}\mathbf{S})\mathbf{z} \quad (24)$$

By identification of the last term in equations (22) and (24), we obtain:

$$\mathbf{Q}^T\mathbf{Q} = (\mathbf{I} - \mathbf{H}\mathbf{S}). \quad (25)$$

Substituting equation (19) into (23), and then (25) into the resulting expressions shows that the χ^2 residual can also be expressed as:

$$q^2 = \mathbf{z}^T (\mathbf{I} - \mathbf{H}\mathbf{S})\mathbf{z} = \mathbf{r}^T \mathbf{r} \quad (26)$$

where the $n \times n$ matrix $(\mathbf{I} - \mathbf{H}\mathbf{S})$ is idempotent and the $n \times 1$ vector \mathbf{r} (defined as $\mathbf{r} \equiv (\mathbf{I} - \mathbf{H}\mathbf{S})\mathbf{z}$) is called the residual vector. Equations (22) to (26) are proof of the equivalence between parity-based and residual-based RAIM [10] [11].

The χ^2 residual q^2 follows a non-central chi square distribution with $(n-m)$ degrees of freedom and non-centrality parameter $\mathbf{f}^T \mathbf{Q}^T \mathbf{Q} \mathbf{f}$. Thus the probability of no detection in equation (18) can be evaluated as:

$$P(q^2 < T^2 | H_i)$$

B. Solution Separation

In contrast with the single test statistic used in χ^2 RAIM, solution separation RAIM employs as many test statistics as fault hypotheses. These test statistics are tailored to the fault hypothesis and to the state of interest [9], and are normally distributed, which is extremely convenient for integrity risk evaluation. The n_H test statistics are defined as:

$$q_i \equiv \varepsilon_0 - \varepsilon_i, \quad i=1, \dots, n_H \quad (27)$$

where the full-set estimate error ε_0 and the fault-free subset estimate error ε_i are respectively defined in (10) to (11) and (14) to (15). In addition [9], [12],

$$q_i = N(\mathbf{s}_{\Delta i}^T \mathbf{f}, \sigma_{\Delta i}^2 \equiv \sigma_i^2 - \sigma_0^2) \quad (28)$$

where $\mathbf{s}_{\Delta i}^T \equiv \mathbf{s}_0^T - [0 \quad \mathbf{s}_i^T]$.

For SS, the probability of no detection, which appears in the integrity risk equation (18) is given by:

$$P\left(|q_1| < T_1, \dots, |q_{n_H}| < T_{n_H} | H_i\right) \quad (29)$$

Similar, the probability of detection in the false-alarm probability equation (3) is also a joint probability. In most practical implementations of SS, the probability in equation (29) is upper-bounded to avoid having to evaluate a joint probability over the n_H correlated random variables q_i . Example probability bounds are derived in Section V.

In addition, it can be shown that $\mathbf{s}_{\Delta i}^T \mathbf{H} = \mathbf{0}$ (see [9] for a complete derivation), which suggests that q_i can be represented in parity space. However, the relationship

between q_i and \mathbf{p} is challenging to establish because solution separations are defined in the position domain.

We can solve this issue for single-measurement faults by first defining failure mode lines: the noise free parity vector ($\mathbf{v} = \mathbf{0}$ in equation (21)) generated by a fault on the i^{th} measurement has a unit direction vector defined as:

$$\mathbf{u}_i \equiv \frac{\mathbf{q}_i}{\sqrt{\mathbf{q}_i^T \mathbf{q}_i}} \quad (30)$$

where \mathbf{q}_i is the i^{th} column of \mathbf{Q} . In parity space, the line passing through the origin with direction vector \mathbf{u}_i is the fault line corresponding to a fault on the i^{th} measurement.

In Appendix I, we provide an analytical proof that for single-measurement faults, the n_H solution separations are projections of the parity vector on their corresponding fault mode lines.

$$q_i = \mathbf{s}_{\Delta i}^T \mathbf{z} = \sigma_{\Delta i} \mathbf{u}_i^T \mathbf{p} \quad (31)$$

The proof in Appendix I uses prior results derived in [9] (including a matrix pseudo-inversion lemma) and is structured in two steps focusing on the faulted measurement, and on the fault-free measurement subset in order to exploit the following observations:

$$\mathbf{s}_{\Delta i}^T \mathbf{A}_i = \mathbf{s}_0^T \mathbf{A}_i \quad \text{and} \quad \mathbf{s}_{\Delta i}^T \mathbf{B}_i = \mathbf{s}_0^T \mathbf{B}_i - \mathbf{s}_i \quad (32)$$

To illustrate this result, we select an example measurement equation, which is then used throughout the paper.

C. Illustrative Example

Let us consider a scalar state x and a 3×1 measurement vector \mathbf{z} defined as:

$$\mathbf{z} = \mathbf{H} x + \mathbf{v} + \mathbf{f} \quad (33)$$

where

$$\mathbf{H} = [1 \quad 1 \quad 1]^T$$

$$\mathbf{v} \sim \mathcal{N}(\mathbf{0}, \mathbf{I})$$

Since $m=1$ and $n=3$, the $(n-m)$ parity space is two-dimensional, which is convenient for display (this example is very similar to the one used by Potter and Suman in [10]). The fault vector \mathbf{f} represents three single-measurement faults (corresponding to three fault hypotheses H_i) with unknown fault magnitude f_i .

$$\mathbf{f} = \begin{bmatrix} f_1 \\ 0 \\ 0 \end{bmatrix} \quad \text{or} \quad \mathbf{f} = \begin{bmatrix} 0 \\ f_2 \\ 0 \end{bmatrix} \quad \text{or} \quad \mathbf{f} = \begin{bmatrix} 0 \\ 0 \\ f_3 \end{bmatrix}$$

These fault models under multiple fault hypotheses is ultimately used in equation (2) to evaluate the integrity risk. As the fault magnitude f_i varies from $-\infty$ to $+\infty$, the noise-free parity vector describes a line in the parity space called the fault mode line, with direction vector \mathbf{u}_i defined in equation (30).

Fig. 1 illustrates equations (23) and (31). The χ^2 residual q is the norm of the parity vector \mathbf{p} , and solution separations q_i , for $i=1, \dots, 3$, are orthogonal projections of \mathbf{p} onto the fault mode lines.

It follows, as illustrated in Fig. 2, that the detection boundaries are a circle for χ^2 , and a polygon for SS. If the SS detection thresholds are all equal ($T_1 = T_2 = T_3$), then the polygon is a hexagon. Detection is established if the parity vector \mathbf{p} derived from \mathbf{z} in equation (19) lands outside the detection boundary.

In conclusion for this section, we have analyzed two detection methods with two different detection boundaries. The difference between a circular and a hexagonal region can appear small, but it is not clear how significant this difference will be in higher dimensional parity space (when additional measurements are available). This difference raises the question: which detection method is best? The answer is sought in Section IV of this paper, where a method is developed to determine the optimal detection region.

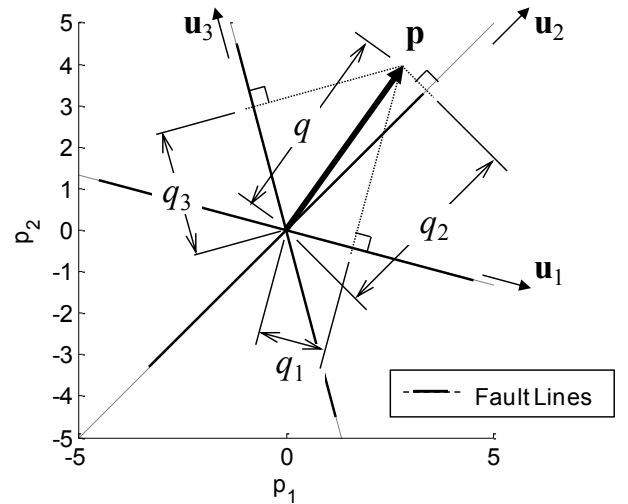


Fig. 1 Detection Test Statistics for χ^2 (q) and SS (q_1, q_2, q_3) in Parity Space

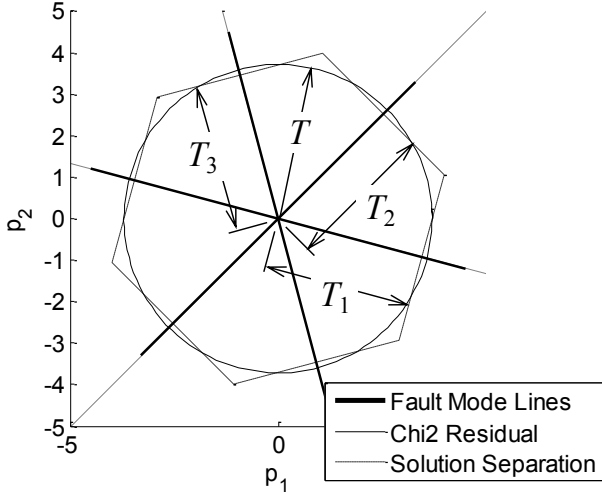


Fig. 2 Detection Boundaries for χ^2 (Circle) and SS (Hexagon) in Parity Space

IV. OPTIMAL PIECEWISE LINEAR DETECTION REGION IN RAIM

A. Optimal Piecewise Linear Detection Boundary

This section presents a method using a piecewise linear boundary to approximate the optimal detection region, which minimizes the integrity risk. Visualizations of the optimal region for varying values of the system requirements will help determine which of χ^2 or SS generates the lowest integrity risk.

The method for building a piecewise linear detection boundary is illustrated in Fig. 3 for the example introduced in Section II-C. The idea is to use extra test statistics in addition to the n_H SS test statistics ($n_H=3$ in Fig. 3). As explained in Section III-B, the SS's are projections of the parity vector on the n_H fault lines represented in gray. We consider additional test statistics, defined as parity vector projections onto lines (in black) that we select at regular angular intervals.

As illustrated with SS in Section II-C, each test statistic generates two segments in the piecewise linear boundary. The higher the number of test statistics is, the finer the resolution of the detection boundary becomes. For clarity of explanation, we consider a total of six test statistics with detection thresholds T_1, \dots, T_6 , as shown in Fig. 3.

It follows that finding the optimal detection boundary narrows down to determining the threshold values T_1, \dots, T_6 that minimize the integrity risk while meeting the false alarm requirement in equation (3).

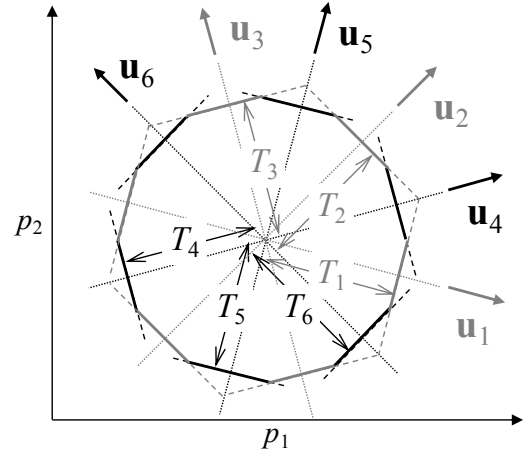


Fig. 3 Piecewise Linear Detection Region Concept

This problem can be formulated as a constrained minimization problem:

$$\min_{T_1, \dots, T_{n_D}} \left\{ \sum_{i=0}^{n_H} \max_{f_i} \left\{ P \left(\begin{array}{l} |\varepsilon_0| > \ell, |q_1| < T_1, \\ \dots, |q_{n_D}| < T_{n_D} \end{array} \middle| H_i, f_i \right) \right\} P_{H_i} \right\} \quad (34)$$

subject to

$$1 - P \left(|q_1| < T_1, \dots, |q_{n_D}| < T_{n_D}, |H_0 \right) P_{H_0} \leq C_{REQO}$$

where n_D is the total number of test statistics ($n_D=6$ in Fig.3). The quantity to minimize in problem statement (34) is a bound on the integrity risk for the worst case fault magnitudes f_i , for $i=1, \dots, n_H$. This worst-case approach is taken because fault magnitudes are extremely difficult to model, especially for rarely occurring faults that are difficult to observe.

Also, in (34), the joint probability of all test statistics being lower than their corresponding thresholds can be computed using one of the following methods:

- directly evaluating the probability of the parity vector being inside the detection boundary: this approach is cumbersome as it involves integrating a multivariate normal distribution (of dimension the length of the parity vector) over the complicated piecewise linear boundary
- stacking all test statistics in an $n_D \times 1$ vector, which follows a multivariate normal distribution whose mean vector and covariance matrix can be computed. In this case, the integration is performed over a hyper-box with edge lengths defined by the thresholds.

- upper-bounding the probability of no detection to facilitate integrity risk evaluation; this approach will be investigated in future work for practical implementations

We select the second of these three options, which was efficiently used in [9] to determine the optimal estimator in RAIM.

The problem formulation in (34) can be modified into an unconstrained minimization problem using the method of Lagrange multipliers (by forcing the inequality constraint to equality), or alternatively, using barrier or penalty methods [13]. The first option is selected here to illustrate the algorithm. Problem (34) becomes:

$$\min_{T_1, \dots, T_{n_d}, \lambda} \left\{ \begin{array}{l} \sum_{i=0}^{n_H} \max_{f_i} \left\{ P \left[\begin{array}{l} |\varepsilon_0| > \ell, |q_1| < T_1, \\ \dots, |q_{n_d}| < T_{n_d} \end{array} \middle| H_i, f_i \right] P_{H_i} \\ + \lambda \left[C_{REQ0} - 1 + P \left[\begin{array}{l} |q_1| < T_1, \dots \\ |q_{n_d}| < T_{n_d}, \end{array} \middle| H_0 \right] \right] \end{array} \right\} \quad (35)$$

where λ is the Lagrange multiplier, to be simultaneously determined with the optimal threshold values.

In the formulation (35), the parameters to be optimized T_1, \dots, T_{n_d} are limits of integration in the objective function. This facilitates the derivation, using the Leibniz integral rule, of analytical expressions for the objective function's gradient vector and Hessian matrix. The main steps of the derivation are given in Appendix II.

An iterative Newton method can then be implemented to determine the optimal parameter values. It converges quickly because the χ^2 threshold T is a good initial guess of the optimal threshold values T_1, \dots, T_{n_d} . However, the rate of convergence can be considerably slowed down by our lack of knowledge on the optimal λ -value. This is why the optimal piecewise linear detection boundary is not intended for practical applications, but is a useful tool to analyze χ^2 and SS methods.

B. Sensitivity to Navigation Requirements

The optimal piecewise linear detection boundary is used to make an educated choice between the χ^2 and SS methods. Consider the illustrative example introduced in Section III.C, with the example parameter values: $P_{H_i} = 10^{-3}$ for $i=1, \dots, 3$, and $C_{REQ0} = 10^{-3}$. The analysis is carried out for a range of values of the non-

dimensional parameter ℓ/σ_0 (which is the ratio of the alert limit over the estimate error standard deviation).

First, the optimal piecewise linear boundary is represented in Fig.4 (thick black lines) for a small value of ℓ/σ_0 ($\ell/\sigma_0=0.3$). Segments of the optimal boundary are of equal length, so that the optimal boundary approaches a circle. This can be observed again in the zoomed-in window on the upper-right hand side of Fig.4, where the optimal boundary is close to the χ^2 circular boundary, and far from the corner of the SS hexagon.

This result is confirmed using another approach based on the Neyman-Pearson (N.P.) theorem [14]. This method provides the means to visualize the optimal no-detection region (gray area in Fig. 4) by determining the set of points in parity space that contribute to reducing the objective function in problem (35). It is again an analytical method, not intended for practical implementations because it involves sampling the parity space point by point.

Thus, the χ^2 method might be selected for $\ell/\sigma_0=0.3$. However, as ℓ/σ_0 increases it is interesting to observe that the optimal detection boundary changes. Fig. 5 shows that for $\ell/\sigma_0=15$, segments of the optimal piecewise linear boundary are no longer equal. The optimal region starts looking like a hexagon, which corresponds to the SS detection boundary. This can be seen again in the zoomed-in window where the optimal N.P. boundary starts filling in the corner of the SS hexagon.

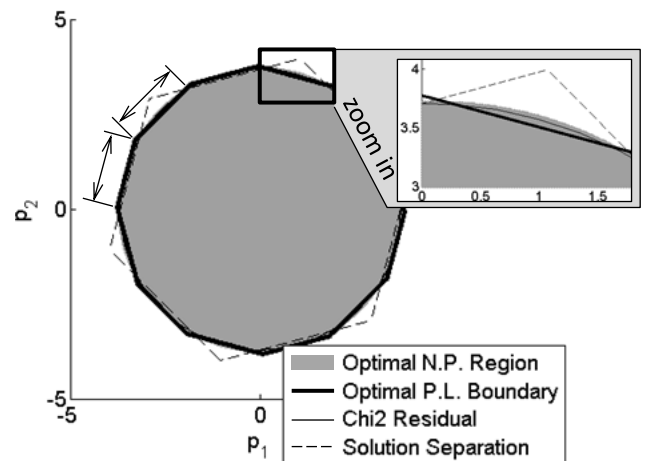


Fig. 4 Optimal Piecewise Linear (P.L.) Detection Boundary for $\ell/\sigma_0 = 0.3$

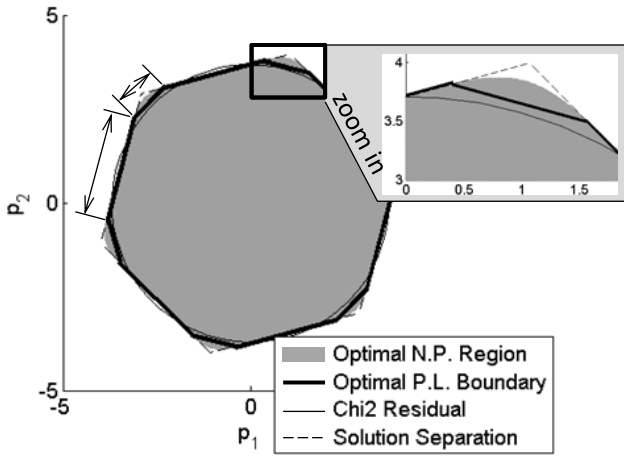


Fig. 5 Optimal Piecewise Linear (P.L.) Detection Boundary for $\ell/\sigma_0 = 15$

To better understand this change in the optimal detection region, we note that two conflicting probability contributions are shaping the optimal detection region as expressed in (35): as the no-detection area increases, the probability of false alarm decreases, but the integrity risk becomes larger. The probability of false alarm is independent of ℓ/σ_0 and is evaluated under the single FF hypothesis, where the parity vector is zero-mean. Therefore, the false alarm requirement defines the minimum surface of an area ‘near the origin’. The optimal area is then shaped by the integrity risk, which is a sum of probabilities over multiple hypotheses, for which the mean parity vector is not zero.

The probability density function for the integrity risk is represented in parity space, in Fig. 6 and 7 for $\ell/\sigma_0 = 0.3$ and $\ell/\sigma_0 = 15$, respectively. In this multiple hypothesis formulation, the density function is a composite of seven peaks of probability density, corresponding to the FF hypothesis, and to the three fault hypotheses for positive and negative values of the fault magnitude.

Fig. 6 shows what appears to be a single peak in probability density because for small values of ℓ/σ_0 , the worst-case fault magnitudes (which maximize the integrity risk) are close to zero, so that the seven peaks are all brought together near the origin. In contrast, as ℓ/σ_0 is increased in Fig. 7, the worst-case fault magnitudes become larger, and the six probability density peaks corresponding to fault hypotheses spread apart along the fault mode lines. It follows that as ℓ/σ_0 increases, the optimal detection boundary changes from a circular area (χ^2) to a polygon (SS).

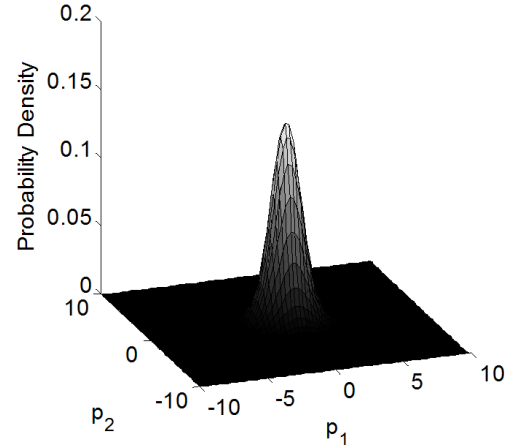


Fig. 6 Density Function of the Probability of HMI for $\ell/\sigma_0 = 0.3$

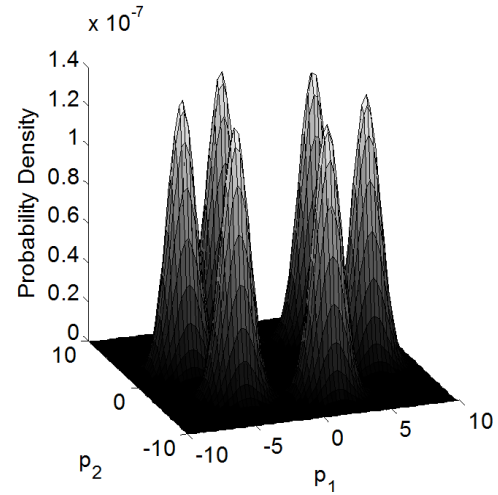


Fig. 7 Density Function of the Probability of HMI for $\ell/\sigma_0 = 15$

Strictly speaking, worst case fault magnitudes depend on the shape of the optimal detection region itself, so that the argument can appear circular. But in practice, we have observed negligibly small variations in worst-case fault magnitudes between the limit cases of χ^2 versus SS. The discussion in the above paragraph captures the dominating trend.

Finally, it should be noticed that the alert limit ℓ must be greater than σ_0 or even the fault-free integrity criterion will not be satisfied. Comparing the scales of the z-axes in Fig. 6 and 7 provides a clue as to the difference in orders of magnitude of P_{HMI} as ℓ/σ_0 changes. Therefore, for most realistic, practical requirements (i.e., for large values of ℓ/σ_0), the optimal detection boundary approaches SS. This result completes and reinforces the findings of previous papers [9], [14]. This is why in the

remainder of this work, we adopt a solution separation approach for fault detection and exclusion (FDE).

V. INTEGRITY AND CONTINUITY RISKS FOR FAULT DETECTION AND EXCLUSION

So far in Sections II to IV, we limited our analysis to fault detection algorithms. For detection only, the detection thresholds are typically set according to a continuity risk allocation C_{REQ0} to limit the probability of false alarms, as expressed in equation (3). However, the complete continuity risk accounts for all events causing a mission to be interrupted. These events include cases of detection under fault-free conditions (false alarms) and of detection under faulted conditions. The continuity risk equation is given by:

$$P_{CONT} = P(D | H_0)P_{H0} + \sum_{i=1}^{n_H} P(D | H_i)P_{Hi} \quad (36)$$

If the detector is efficient, then the second term on the right hand side of (36) is close to the prior probability of any fault occurring:

$$\sum_{i=1}^{n_H} P(D | H_i)P_{Hi} \approx \sum_{i=1}^{n_H} P_{Hi} \quad (37)$$

If this probability is larger than the overall continuity risk requirement C_{REQ} , then faults need to be excluded to continue using the system.

This is why fault exclusion algorithms have been derived and implemented [4], [5], [6]. One crucial element that is currently missing in the literature, and that has been described as missing in [7] and [8], is a rigorous derivation of the integrity risk and continuity risk for RAIM FDE.

The objective of this section is to address this issue. The derivation starts with a redefinition of the integrity risk equation for fault detection *and exclusion*:

$$P_{HMI} \equiv \sum_{i=0}^{n_H} P(HI, ND | H_i)P_{Hi} + \sum_{i=0}^{n_H} \sum_{j=1}^{n_H} P(HI, D, E_j | H_i)P_{Hi} \quad (38)$$

where

- HI : hazardous information
- ND : no detection
- D : detection
- E_j : exclusion of measurement subset j

The first term in equation (38) is the same as the integrity risk for detection only given in equation (2). The second term accounts for the risk when excluding: it is the price we have to pay in terms of integrity risk for reducing the continuity risk using exclusion. It accounts for all fault hypotheses (subscript i), all ‘exclusion hypotheses’ (subscript j).

In parallel, the continuity risk is redefined to express that mission interruptions occur if a fault is detected, but cannot be excluded:

$$P_{CONT} \equiv \sum_{i=0}^{n_H} P(D, NE | H_i)P_{Hi} \quad (39)$$

where

NE : no exclusion

To understand how no-exclusion events can occur, we present an example four-step SS exclusion procedure:

- 1) First, we check whether the SS detection tests pass or not. As described in Sections III and IV, a fault is detected if:

$$|\varepsilon_0 - \varepsilon_k| \geq T_k \quad \text{for any } k, k=1, \dots, n_H \quad (40)$$

- 2) In case of detection, we choose a measurement subset ‘ j ’ to exclude. This work does not address how this choice is made. Instead, this work considers all exclusion hypotheses, so that the integrity risk equation is valid for *any* excluded measurement subset j .

- 3) Next, we make sure that the selected subset solution ε_j (using all remaining measurements after exclusion) is fault free. We carry out a second layer of detection using all subset solutions $\varepsilon_{j,l}$ within the selected subset solution ε_j . Thus, a subset ‘ j ’ is excluded only if

$$|\varepsilon_j - \varepsilon_{j,l}| < T_{j,l} \quad \forall l, \begin{cases} l=1, \dots, n_H \\ l \neq j \end{cases} \quad (41)$$

This amounts to a number of $n_H - 1$ exclusion tests per fault hypothesis.

- 4) Finally, if any one of these exclusion tests triggers (i.e., if the selected subset solution ε_j is inconsistent), then the mission is interrupted. This case must be accounted for in the continuity risk equation.

These four steps and the general definitions of integrity and continuity risks in equations (38) and (39) are used in Sections V-A and V-B to derive expressions of P_{HMI} and P_{CONT} for FDE using the SS RAIM method. This derivation remains valid for estimators other than the least squares estimator and is not restricted to single measurement faults.

A. Integrity Risk Equation for SS ARAIM FDE

The actual integrity risk is extremely difficult to evaluate because the estimate errors ε_j and the detection and exclusion test statistics are correlated. Instead, in Appendix III of this paper, we establish an upper bound on P_{HMI} , which is derived to enable integrity risk evaluation in practical implementations. The integrity risk bound is expressed as:

$$\begin{aligned}
P_{HMI} \leq & P(|\varepsilon_0| > \ell \mid H_0)P_{H0} \\
& + \sum_{i=1}^{n_H} P(|\varepsilon_i| + T_i > \ell \mid H_i)P_{Hi} \\
& + \sum_{i=1}^{n_H} P(|\varepsilon_i| > \ell \mid H_i)P_{Hi} \\
& + \sum_{j=1}^{n_H} P(|\varepsilon_j| > \ell \mid H_0)P_{H0} \\
& + \sum_{i=1}^{n_H} \sum_{\substack{j=1 \\ j \neq i}}^{n_H} P(|\varepsilon_{j,i}| + T_{j,i} > \ell \mid H_i)P_{Hi}
\end{aligned} \quad (42)$$

The first two terms on the right hand side (RHS) of equation (42) are a bound on the probability of hazardous information and no detection. The equivalent protection level formulation for these terms is typically used for integrity risk evaluation in SS RAIM using detection only [2] [7].

The next three terms on the RHS of (42) account for all cases of hazardous information, detection, and exclusion. The third, fourth, and fifth terms are respectively bounds on the probability of correct exclusion, of wrong exclusion under FF conditions, and of wrong exclusion under faulty conditions.

Unlike the second, third and fifth terms, the fourth term is multiplied by P_{H0} , which is close to one. In case this bound is too loose and causes loss of availability, an alternative bound is provided in Appendix III: this alternate bound is a function of the continuity risk allocation over which we have some control (see Appendix III for additional details). The alternate bound was not needed in performance evaluations of Section VI.

Again, the integrity risk bound in equation (42) was designed to enable risk evaluation in cases where computational resources are limited. This bound can also be expressed in the simple form of protection level (PL) equations:

$$\begin{aligned}
PL_{ND,0} &= k_{ND,0} \sigma_0 \\
PL_{ND,i} &= k_{ND,i} \sigma_i + T_i \\
PL_{CE,i} &= k_{CE,i} \sigma_i \\
PL_{WE,0,j} &= k_{WE,0,j} \sigma_j \\
PL_{WE,j,i} &= k_{WE,j,i} \sigma_{j,i} + T_{j,i}
\end{aligned} \quad (43)$$

where

$$\begin{aligned}
k_{ND0} &= Q^{-1}\{I_{REQND0}/(2P_{H0})\} \\
k_{ND,i} &= Q^{-1}\{I_{REQND,i}/(2P_{Hi})\} \\
k_{CE,i} &= Q^{-1}\{I_{REQCE,i}/(2P_{Hi})\} \\
k_{WE,0,j} &= Q^{-1}\{I_{REQWE,0,j}/(2P_{H0})\} \\
k_{WE,j,i} &= Q^{-1}\{I_{REQWE,j,i}/(2P_{Hi})\}
\end{aligned}$$

and $\sigma_{j,i}$ is the standard deviation of the subset solution that excludes both the i and j measurement subsets. The function $Q^{-1}\{\}$ is the inverse tail probability distribution of the two-tailed standard normal distribution ($Q\{\}=1-\Phi\{\}$, where $\Phi\{\}$ is the standard normal cumulative distribution function).

The price to pay to obtain simple PL expressions in equation (43) as compared to (42) is that the integrity risk must be allocated among all the terms. This can result in a looser integrity risk bound, which may ultimately impact navigation availability. In equation (43), the probability multipliers or k -values are computed for predefined integrity risk requirement allocations I_{REQND0} ,

$$I_{REQND,i}, I_{REQCE,i}, I_{REQWE,0,j}, I_{REQWE,j,i}.$$

The overall PL, which is compared to the alert limit ℓ to check whether navigation requirements are satisfied or not, is given by:

$$PL = \max(PL_{ND,0}, PL_{ND,i}, PL_{CE,i}, PL_{WE,0,j}, PL_{WE,j,i}) \quad (44)$$

On a parenthetical note, the ARAIM implementation illustrated in Section VI assumes non-zero mean measurement errors, with nominal biases not exceeding the value b_{MAX} . In this case the following terms must be added in the PL equations (43):

- $\sum_{l=1}^n |s_{0,l}| b_{MAX}$ in the first equation
- $\sum_{l=1}^{n-n_i} |s_{i,l}| b_{MAX}$ in the second and third equations
- $\sum_{l=1}^{n-n_j} |s_{j,l}| b_{MAX}$ in the fourth equation
- $\sum_{l=1}^{n-n_i-n_j} |s_{ji,l}| b_{MAX}$ in the fifth equation

where $s_{i,l}$ is the l^{th} element of \mathbf{s}_i , and in the fifth equation, $s_{ji,l}$ are elements of \mathbf{s}_{ji} , which is the least squares estimator vector for the state of interest, for the subset solution that excludes subsets i and j , comprising n_i and n_j measurements, respectively.

B. Continuity Risk Equation for SS ARAIM FDE

In Appendix IV of this paper, a bound on the continuity risk P_{CONT} is derived, which is expressed as:

$$P_{CONT} \leq \sum_{i=1}^{n_H} \left(P(|\varepsilon_i - \varepsilon_0| \geq T_i | H_0) P_{H_0} + \sum_{\substack{j=1 \\ j \neq i}}^{n_H} P(|\varepsilon_{j,i} - \varepsilon_j| \geq T_{j,i} | H_0) P_{H_i} \right) \quad (45)$$

This equation is crucial because it provides the means to determine the n_H detection thresholds and the $n_H(n_H - 1)$ exclusion thresholds, while ensuring that the overall continuity risk requirement C_{REQ} is met.

To achieve this, one straightforward approach is simply to allocate the continuity risk requirement to each one of the terms in equation (45). An example allocation is given as follows:

- Allocation between fault hypotheses

$$C_{REQ} = \sum_{i=1}^{n_H} C_{REQ_i} \quad (46)$$

where, for example, $C_{REQ_i} = C_{REQ}/n_H$

- Allocation between detection and exclusion terms:

$$C_{REQ_i} = (\beta + (1 - \beta)) C_{REQ_i} \quad (47)$$

where $0 < \beta \leq 1$, e.g., $\beta = 1/2$

- Allocation between exclusion hypotheses :

$$(1 - \beta) C_{REQ_i} = (1 - \beta) C_{REQ_i} \sum_{j=1}^{n_H-1} \alpha_{j,i} \quad (48)$$

where $\sum_{j=1}^{n_H-1} \alpha_{j,i} = 1$, e.g., $\alpha_{j,i} = 1/(n_H - 1)$

Therefore, we want the detection and exclusion thresholds to satisfy the following inequalities:

$$P(|\varepsilon_i - \varepsilon_0| \geq T_i | H_0) \leq \beta C_{REQ_i} / P_{H_0} \quad (49)$$

$$P(|\varepsilon_{j,i} - \varepsilon_j| \geq T_{j,i} | H_0) \leq \alpha_{j,i} (1 - \beta) C_{REQ_i} / P_{H_i} \quad (50)$$

from which we obtain:

$$T_i = Q^{-1} \left\{ \beta \frac{C_{REQ_i}}{2P_{H_0}} \right\} \sigma_{\Delta_i} \quad (51)$$

$$T_{j,i} = Q^{-1} \left\{ \alpha_{j,i} (1 - \beta) \frac{C_{REQ_i}}{2P_{H_i}} \right\} \sigma_{\Delta_{j,i}} \quad (52)$$

where σ_{Δ_i} is defined in equation (28) and $\sigma_{\Delta_{j,i}}$ is the standard deviation of $\varepsilon_{j,i} - \varepsilon_j$. $\sigma_{\Delta_{j,i}}$ can be computed as $\sigma_{\Delta_{j,i}}^2 = \sigma_{j,i}^2 - \sigma_j^2$, where σ_j^2 and $\sigma_{j,i}^2$ are respectively defined in (15) and (43).

It is worth noticing that the number of thresholds to determine in equation (45) is n_H^2 . To shed some light on this number, we represent the SS FDE algorithm in parity space.

C. ARAIM FDE Parity Space Representation

The no-detection and exclusion regions can be visualized in parity space by sampling the parity space and figuring out which points pass the detection and exclusion tests outlined in the above four-step procedure for SS RAIM FDE. For the illustrative example introduced in Section III-C, we recognize the hexagonal no-detection zone displayed in fair gray in Fig.8.

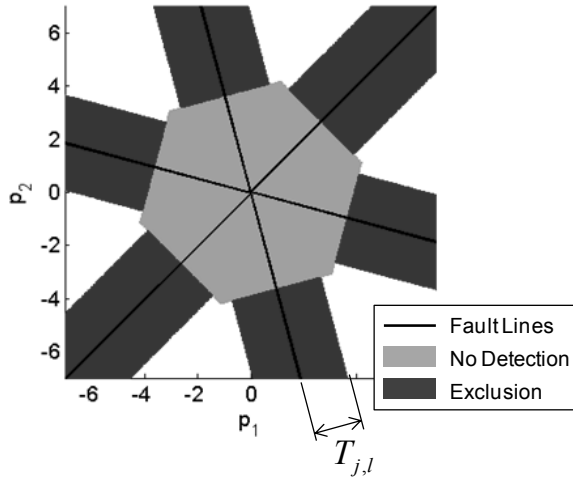


Fig. 8 Detection and Exclusion Zones in Two Dimensional Parity Space

The SS exclusion areas (dark gray) turn out to be bands surrounding the fault mode lines. A band-shaped area for each fault hypothesis was not obvious to infer from the $n_H - 1$ exclusion tests in equation (41). But these bands are sensible criteria for exclusion. If the parity vector is near a fault mode, then it is easy to deduce which measurement to exclude. On the contrary, if the parity vector lands in between two fault mode lines, then it becomes extremely challenging to determine which of the two fault modes caused the error that was detected. And, a more stringent exclusion criterion is obtained by simply reducing the exclusion thresholds $T_{j,l}$.

It is noteworthy that the exclusion regions have piecewise linear boundaries. We can therefore use a similar optimization procedure to that described in Section IV, which provides values of the detection and exclusion thresholds that minimize the integrity risk (instead of using the arbitrary allocation of Section V-B). The optimal piecewise linear exclusion regions are shown in Fig. 9 (gray areas), in comparison with the boundaries (dashed black lines) resulting from the arbitrary continuity risk allocation given in equations (46) to (48). Of interest in this example is the fact that the optimization process reduces areas of overlapping exclusion zones: these areas are actually counted twice in the integrity risk bound in equation (42), as a result of the tradeoff that was made in Appendix III between tightness of the bounds on P_{CONT} and P_{HMI} versus computational efficiency.

One singular aspect of the SS approach is that it requires $n_H - 1$ exclusion test statistics to generate a band-shape zone along the fault line. The same exclusion performance could be obtained using a single test statistic measuring the distance from the fault line.

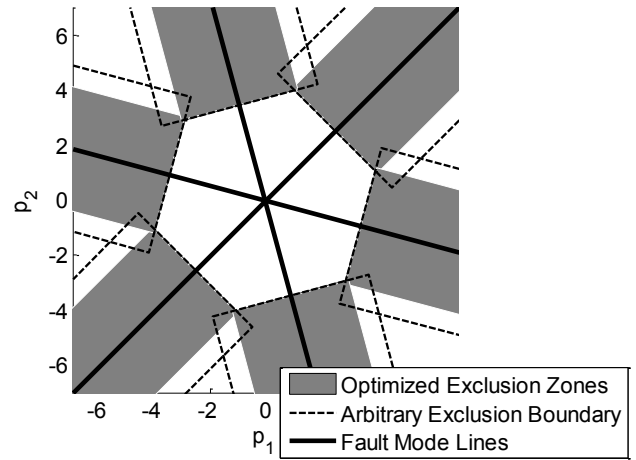


Fig. 9 Optimal Piecewise Linear Exclusion Boundaries in Parity Space

To bring some insight to this apparently unnecessarily-large number of tests, the exclusion regions are represented in higher-dimensional parity space. For example, to obtain a three-dimensional parity space representation, the measurement vector \mathbf{z} in equation (33) is augmented with one additional measurement, so that the observation matrix becomes:

$$\mathbf{H} = [1 \ 1 \ 1 \ 1]^T \quad (53)$$

The 4×1 measurement noise vector \mathbf{v} is still zero-mean normally distributed with covariance \mathbf{I} and the 4×1 fault vector now includes one additional single-measurement fault mode.

The resulting no-detection and exclusion spaces are respectively shown in fair gray and dark gray in Fig. 10. Focusing on a single fault mode and looking at a plane normal to the corresponding fault mode line reveals the shape of the SS exclusion region, which is displayed in Fig. 11. If a single test statistic measuring the Euclidean distance to the fault mode line was used for exclusion, then the exclusion boundary would be circular, and the test statistic would follow a non-central chi-square distribution. Instead, SS uses multiple test statistics that measure parity vector projections, and allows to preserve normally-distributed test statistics. Dealing with normally-distributed variables is extremely convenient for practical risk evaluation as highlighted Sections V-A and V-B and in Appendices III and IV.

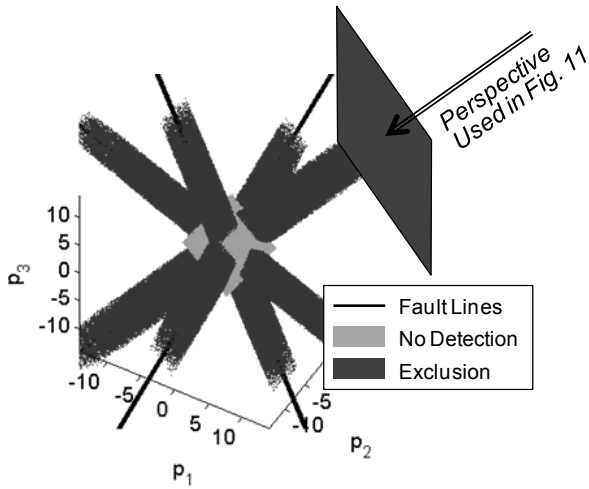


Fig. 10 Detection and Exclusion Zones in Three Dimensional Parity Space

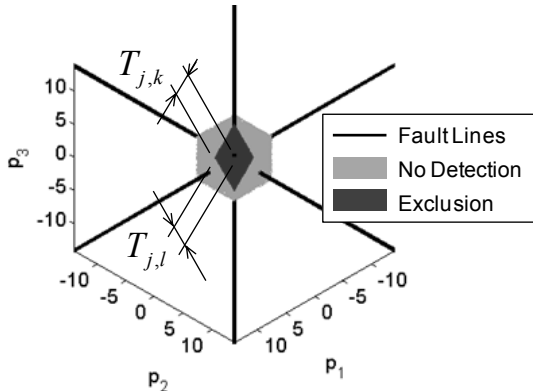


Fig. 11 Visualizing the Exclusion Region

Finally, the exclusion region surprisingly turns out to be diamond-shaped. The same observation was made using more realistic measurement equations (e.g., using seven GPS ranging measurement to estimate three position coordinates and one receiver clock state): as the satellite geometry was changed, the exclusion region remained a diamond. This raises a question, as it did in Section III: what is the shape of the optimal exclusion region? This question is left open for future work.

V. BENCHMARK APPLICATION: AIRCRAFT APPROACH USING MULTI-CONSTELLATION GNSS

This section presents a performance evaluation of Advanced RAIM (ARAIM) for worldwide vertical guidance of aircraft using dual-frequency GPS and Galileo. As mentioned in Section I, when using redundant satellite signals from two constellations instead of one, the RAIM detection capability increases considerably, but the probability of satellite failures increases. In multi-constellation implementations, measurement exclusion is crucial to maintain a high level of continuity.

Table 1. Simulation Parameters

Description	Value
SV clock and orbit error (URA)	0.75 m (0.957 m for Galileo)
Residual tropospheric error *	$0.12 \frac{1.001}{(0.002001 + \sin^2 \xi)^{1/2}}$ m
Smoothed code multipath *	$0.13 + 0.53e^{-\xi/10}$ m (lookup table for Galileo [3])
Smoothed code receiver noise *	$0.15 + 0.43e^{-\xi/6.9}$ m
Fault-free meas. bias b_{MAX}	0.75 m (1 m for Galileo)
Integrity risk requirement	10^{-7}
Continuity risk requirement C_{REQ}	$2 \cdot 10^{-6}$
Prior probability of satellite fault P_{Hi}	10^{-5}
Prior probability of constellation fault	none considered
*: ξ is the satellite elevation angle in degrees.	

The integrity risk and continuity risk bounds in equations (42) and (45) are used to quantify availability. We use the continuity risk allocation outlined in Section V-B (with $\beta = 0.01$) to determine the exclusion and detection thresholds. The simulation parameters, which include ARAIM measurement error and single-satellite fault models, and LPV-200 navigation requirements (to support localizer precision vertical aircraft approach operations down to 200 feet above the ground), are summarized in Table 1 and described in detail in [3]. We assume a ‘24-1’ GPS satellite constellation and a ‘27-1’ Galileo constellation, which are nominal constellations with one spacecraft removed to account for outages; these example constellations are also described in detail [3]. Moreover, this analysis focuses on the vertical position coordinate, for which the aircraft approach navigation requirements are often the most difficult to fulfill. In this case, the target vertical alert limit (VAL), noted ℓ in all the above equations, is 35 m.

Figures 12, 13 and 14 compare availability maps respectively generated for VAL of 20m, 25m and 35m, for a 10 deg \times 10 deg grid of locations. Availability is color-coded from black to white representing availability values ranging from 90% to 100%, respectively. As expected, the maps show that availability decreases as

VAL is tightened, but for the target VAL of 35m, availability averaged over all locations is 100%. These availability maps include both detection and exclusion. Fig. 14 not only shows that the integrity risk and false alarm requirements can be met, which would be the extent of the analysis using detection only. But, beyond this, it also demonstrates that the overall continuity risk requirement can be satisfied, and with high availability.

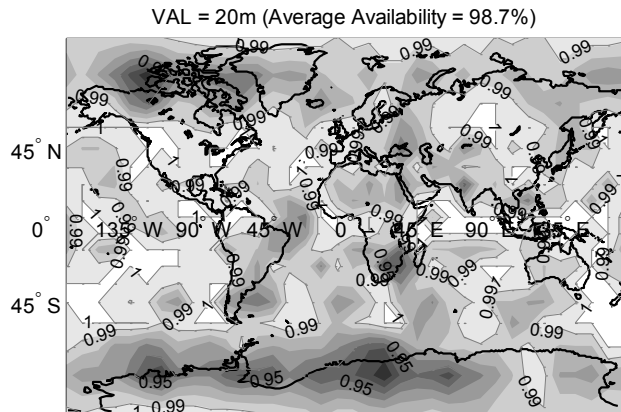


Fig. 12 Availability for VAL = 20 m

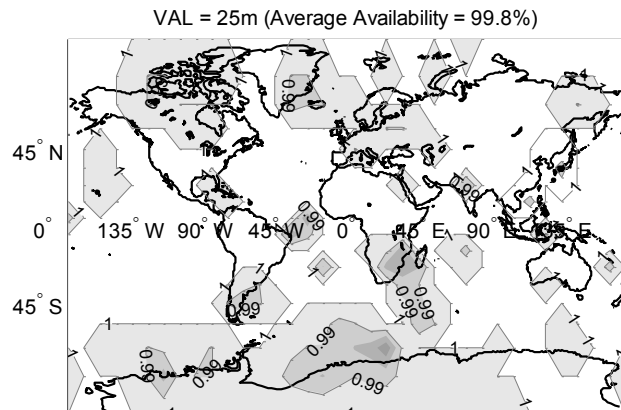


Fig. 13 Availability for VAL = 25 m

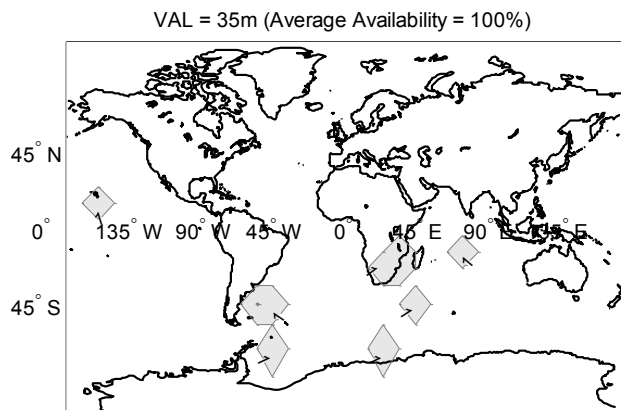


Fig. 14 Availability for VAL = 35 m

VI. CONCLUSION

This paper introduced new methods to analyze and evaluate the integrity and continuity performance of RAIM-based fault detection and exclusion (FDE).

First, parity space representations were used to analyze the performance of solution separation (SS) Advanced RAIM (ARAIM). The SS test statistics were proved to be projections of the parity vector on failure mode lines. Thus, the SS detection boundary could be represented as a polytope. A method was established to visualize the optimal detection region, which, for most realistic, practical requirements, was shown to match the polytope-shaped SS boundary. Parity space representations of the exclusion regions further reaffirmed the practical benefit of SS ARAIM for risk evaluation based on normally-distributed SS test statistics.

Second, we developed integrity risk and continuity risk bounds for SS RAIM FDE. The integrity risk bound (or alternatively, the proposed protection level) was designed for computationally-efficient risk evaluation. The continuity risk bound enables threshold determination for detection and exclusion while satisfying the overall continuity risk requirement. Equations (42) (or 43) and (45) (or (51) and (52)) provide the means to not only evaluate the integrity risk and false alarm probability, but also to quantify the overall continuity risk using fault exclusion.

Performance assessment using these new methods was carried out for an example aircraft approach navigation application, and showed high availability of integrity and continuity despite taking into account the risk of wrong exclusions.

APPENDIX I. PROOF THAT NORMALIZED SOLUTION SEPARATIONS ARE PROJECTIONS OF THE PARITY VECTOR ON FAULT MODE LINES

This appendix presents a proof that the n_H solution separations are projections of the parity vector on their corresponding single-measurement fault mode lines. In mathematical form, we present a derivation for equation (31), which is rewritten as:

$$\frac{s_{\Delta i}^T}{\sigma_{\Delta i}} \mathbf{z} = \frac{\mathbf{q}_i^T}{\sqrt{\mathbf{q}_i^T \mathbf{q}_i}} \mathbf{Q} \mathbf{z} \quad (\text{A.1})$$

To simplify the notations and without loss of generality (because the order in which measurements are stacked in \mathbf{z} is arbitrary), consider a fault on the first measurement. Equation (13) becomes:

$$\mathbf{A}_i = \begin{bmatrix} 1 \\ \mathbf{0} \end{bmatrix} \quad \text{and} \quad \mathbf{B}_i = \begin{bmatrix} \mathbf{0} \\ \mathbf{I}_{n-1} \end{bmatrix} \quad (\text{A.2})$$

and the $(n-m) \times 1$ vector \mathbf{q}_i in equation (A.1) becomes:

$$\mathbf{q}_i = \mathbf{Q}\mathbf{A}_i \quad (\text{A.3})$$

For clarity of exposition, this appendix focuses on a single fault hypothesis, and subscript ‘ i ’ is dropped.

In addition, let us modify the following notations, for consistency with [9]:

- For the full-set solution in equations (6) to (11)

$$\mathbf{P} \equiv \mathbf{P}_0, \quad \mathbf{S} \equiv \mathbf{S}_0, \quad \mathbf{s} \equiv \mathbf{s}_0, \quad \sigma \equiv \sigma_0 \quad (\text{A.4})$$

- For the fault-free subset solution in equations (14) to (17)

$$\mathbf{P}_B \equiv \mathbf{P}_i, \quad \mathbf{S}_B \equiv \mathbf{S}_i, \quad \mathbf{s}_B \equiv \mathbf{s}_i, \quad \sigma_B \equiv \sigma_i \quad (\text{A.5})$$

- For the single faulted measurement

$$\mathbf{H}_A = \mathbf{A}^T \mathbf{H} \quad (\text{A.6})$$

- For the solution separation in equation (28)

$$\mathbf{S}_\Delta = \mathbf{S}_0 - \mathbf{S}_i$$

The measurement vector can be broken down into two components corresponding to the faulted measurement, and to the fault-free measurement subset, following the equation:

$$\mathbf{z} = (\mathbf{A}\mathbf{A}^T + \mathbf{B}\mathbf{B}^T) \mathbf{z}, \quad (\text{A.7})$$

Substituting (A.3) and (A.7) into (A.1) shows that the proof of equation (A.1) can be given in two steps:

- $$\frac{\mathbf{s}_\Delta^T}{\sigma_\Delta} \mathbf{A} = \frac{\mathbf{A}^T \mathbf{Q}^T \mathbf{Q} \mathbf{A}}{\sqrt{\mathbf{A}^T \mathbf{Q}^T \mathbf{Q} \mathbf{A}}} = (\mathbf{A}^T \mathbf{Q}^T \mathbf{Q} \mathbf{A})^{\frac{1}{2}} \quad (\text{A.8})$$

- $$\frac{\mathbf{s}_\Delta^T}{\sigma_\Delta} \mathbf{B} = \frac{\mathbf{A}^T \mathbf{Q}^T \mathbf{Q} \mathbf{B}}{\sqrt{\mathbf{A}^T \mathbf{Q}^T \mathbf{Q} \mathbf{A}}} \quad (\text{A.9})$$

Step 1: Proof for (A.8)

It was shown in [9] that:

$$\mathbf{P}_B^{-1} = \mathbf{P}^{-1} - \mathbf{H}_A^T \mathbf{V}_A^{-1} \mathbf{H}_A \quad (\text{A.10})$$

The first three equations of this derivation (A.11) to (A.13) were already given in [9]. The variance of the fault-free subset solution can be expressed as (by substituting equation (A.5) into (15)):

$$\begin{aligned} \sigma_B^2 &= \boldsymbol{\alpha}^T \mathbf{P}_B \boldsymbol{\alpha} \\ &= \boldsymbol{\alpha}^T (\mathbf{P}^{-1} - \mathbf{H}_A^T \mathbf{H}_A)^{-1} \boldsymbol{\alpha} \end{aligned} \quad (\text{A.11})$$

Using the matrix inversion identity (also known as Woodbury’s formula), equation A.11 becomes:

$$\begin{aligned} \sigma_B^2 &= \boldsymbol{\alpha}^T (\mathbf{P} + \mathbf{P} \mathbf{H}_A^T (\mathbf{I} - \mathbf{H}_A \mathbf{P} \mathbf{H}_A^T)^{-1} \mathbf{H}_A \mathbf{P}) \boldsymbol{\alpha} \\ &= \sigma^2 + \boldsymbol{\alpha}^T \mathbf{P} \mathbf{H}_A^T (\mathbf{I} - \mathbf{H}_A \mathbf{P} \mathbf{H}_A^T)^{-1} \mathbf{H}_A \mathbf{P} \boldsymbol{\alpha} \\ &= \sigma^2 + \mathbf{s}^T \mathbf{A} (\mathbf{A}^T (\mathbf{I} - \mathbf{H} \mathbf{S}) \mathbf{A})^{-1} \mathbf{A}^T \mathbf{s} \end{aligned} \quad (\text{A.12})$$

An expression of the solution separation’s variance is obtained:

$$\sigma_\Delta^2 = \sigma_B^2 - \sigma^2 = \mathbf{s}^T \mathbf{A} (\mathbf{A}^T (\mathbf{I} - \mathbf{H} \mathbf{S}) \mathbf{A})^{-1} \mathbf{A}^T \mathbf{s} \quad (\text{A.13})$$

Since in this appendix, \mathbf{A} is a $n \times 1$ vector, the term under the inversion is a scalar. Also, equation (25) shows that it is derived from an inner product of a vector with itself, and hence it is a positive scalar. Thus, the standard deviation of the solution separation can be written as:

$$\sigma_\Delta = \mathbf{s}^T \mathbf{A} (\mathbf{A}^T (\mathbf{I} - \mathbf{H} \mathbf{S}) \mathbf{A})^{-\frac{1}{2}} \quad (\text{A.14})$$

Substituting equation (25) into (A.14) results in:

$$\sigma_\Delta = \mathbf{s}^T \mathbf{A} (\mathbf{A}^T \mathbf{Q}^T \mathbf{Q} \mathbf{A})^{\frac{1}{2}} \quad (\text{A.15})$$

In addition, substituting equation (32) (i.e., $\mathbf{s}_\Delta^T \mathbf{A} = \mathbf{s}^T \mathbf{A}$) into (A.14), we obtain an expression that is equivalent to (A.8), which concludes ‘Step 1’:

$$\sigma_\Delta = \mathbf{s}_\Delta^T \mathbf{A} (\mathbf{A}^T \mathbf{Q}^T \mathbf{Q} \mathbf{A})^{\frac{1}{2}} \quad (\text{A.16})$$

Step 2: Proof for (A.9)

Multiplying both sides of (A.9) by $(\mathbf{A}^T \mathbf{Q}^T \mathbf{Q} \mathbf{A})^{1/2}$ and substituting (A.8) for $(\mathbf{A}^T \mathbf{Q}^T \mathbf{Q} \mathbf{A})^{1/2}$ into the resulting expression yields the following equation:

$$\mathbf{A}^T \frac{\mathbf{S}_\Delta \mathbf{S}_\Delta^T}{\sigma_\Delta^2} \mathbf{B} = \mathbf{A}^T \mathbf{Q}^T \mathbf{Q} \mathbf{B} \quad (\text{A.17})$$

In addition, the second section of Appendix II of [9] shows that:

$$\mathbf{A}^T \mathbf{S}_\Delta^T \mathbf{P}_\Delta^+ \mathbf{S}_\Delta \mathbf{B} = \mathbf{A}^T (\mathbf{I} - \mathbf{H} \mathbf{S}) \mathbf{B} \quad (\text{A.18})$$

where \mathbf{P}_Δ^+ is the Moore-Penrose pseudo-inverse of \mathbf{P}_Δ ($\mathbf{P}_\Delta = \mathbf{P}_B - \mathbf{P}_0$). Under the single-satellite fault assumption, \mathbf{P}_Δ is of rank 1. Thus, the normalization operation using \mathbf{P}_Δ^+ in the left hand side of equation (A.18) can be performed using any (non-zero) scalar element of \mathbf{P}_Δ . In particular, for the state of interest, we have:

$$\mathbf{S}_\Delta^T \mathbf{P}_\Delta^+ \mathbf{S}_\Delta = \mathbf{S}_\Delta^T \frac{\boldsymbol{\alpha} \boldsymbol{\alpha}^T}{\sigma_\Delta^2} \mathbf{S}_\Delta \quad (\text{A.19})$$

Finally, substituting equations (A.19) and (25) into (A.18) results in equation (A.17), which concludes the proof for this appendix.

APPENDIX II. GRADIENT AND HESSIAN OF THE OBJECTIVE FUNCTION FOR THE MINIMIZATION PROBLEM IN EQUATION (34)

In this appendix we provide the main steps of the gradient vector and Hessian matrix derivation, which are important to efficiently solve the constrained minimization problem in equation (34) using in a Newton method.

Several methods can be used to enforce the constraint by incorporating the constraint equation in the objective function [13]. The terms derived in this appendix for a simplified objective function θ appear in all methods. The same basic terms also appear in the integrity risk minimization problem for fault exclusion in Section V. The simplified objective function is expressed as:

$$\theta(T_1, T_2, T_3) = \int_{-T_3}^{T_3} \int_{-T_2}^{T_2} \int_{-T_1}^{T_1} \phi(q_1, q_2, q_3) dq_1 dq_2 dq_3 \quad (\text{A.20})$$

where q_1 , q_2 , and q_3 are correlated random variables (representing the detection test statistics in equation (35)), and ϕ is the probability density function for a non-zero mean multivariate normal distribution.

For the minimization problem over detection thresholds T_1 , T_2 , T_3 , the elements of the gradient vector can be expressed, using the Leibniz integral rule, as:

$$\begin{aligned} \frac{\partial \theta(T_1, T_2, T_3)}{\partial T_1} &= \int_{-T_3}^{T_3} \int_{-T_2}^{T_2} \phi(T_1, q_2, q_3) dq_2 dq_3 \\ &+ \int_{-T_3}^{T_3} \int_{-T_2}^{T_2} \phi(-T_1, q_2, q_3) dq_2 dq_3 \end{aligned} \quad (\text{A.21})$$

The expression in (A.21) cannot easily be evaluated. Let ζ be an infinitesimally small number. Equation (A.21) can be rewritten and approximated as:

$$\begin{aligned} \frac{\partial \theta(T_1, T_2, T_3)}{\partial T_1} &= \lim_{\zeta \rightarrow 0} \frac{1}{\zeta} \left[\int_{-T_3}^{T_3} \int_{-T_2}^{T_2} \int_{T_1 - \zeta/2}^{T_1 + \zeta/2} \phi(q_1, q_2, q_3) dq_1 dq_2 dq_3 \right. \\ &\quad \left. + \int_{-T_3}^{T_3} \int_{-T_2}^{T_2} \int_{-T_1 - \zeta/2}^{-T_1 + \zeta/2} \phi(q_1, q_2, q_3) dq_1 dq_2 dq_3 \right] \\ &\approx \frac{1}{\zeta} \left[\int_{-T_3}^{T_3} \int_{-T_2}^{T_2} \int_{T_1 - \zeta/2}^{T_1 + \zeta/2} \phi(q_1, q_2, q_3) dq_1 dq_2 dq_3 \right. \\ &\quad \left. + \int_{-T_3}^{T_3} \int_{-T_2}^{T_2} \int_{-T_1 - \zeta/2}^{-T_1 + \zeta/2} \phi(q_1, q_2, q_3) dq_1 dq_2 dq_3 \right] \end{aligned}$$

The above expression enables the use of existing numerical methods [15] to evaluate the right hand side's cumulative distribution functions for the vector of correlated random variables $[q_1 \ q_2 \ q_3]^T$.

The same method is used to determine the off-diagonal and diagonal elements of the gradient matrix, which are respectively expressed as:

$$\begin{aligned} \frac{\partial \theta(T_1, T_2, T_3)}{\partial T_1 \partial T_2} &= \int_{-T_3}^{T_3} \int_{T_2 - \zeta/2}^{T_2 + \zeta/2} \int_{T_1 - \zeta/2}^{T_1 + \zeta/2} \phi(q_1, q_2, q_3) dq_1 dq_2 dq_3 \\ &+ \int_{-T_3}^{T_3} \int_{-T_2 - \zeta/2}^{-T_2 + \zeta/2} \int_{T_1 - \zeta/2}^{T_1 + \zeta/2} \phi(q_1, q_2, q_3) dq_1 dq_2 dq_3 \\ &+ \int_{-T_3}^{T_3} \int_{T_2 - \zeta/2}^{T_2 + \zeta/2} \int_{-T_1 - \zeta/2}^{-T_1 + \zeta/2} \phi(q_1, q_2, q_3) dq_1 dq_2 dq_3 \\ &+ \int_{-T_3}^{T_3} \int_{-T_2 - \zeta/2}^{-T_2 + \zeta/2} \int_{-T_1 - \zeta/2}^{-T_1 + \zeta/2} \phi(q_1, q_2, q_3) dq_1 dq_2 dq_3 \end{aligned}$$

$$\frac{\partial^2 \theta(T_1, T_2, T_3)}{\partial T_1^2} \approx \frac{1}{\zeta^2} \begin{bmatrix} \int_{-T_3}^{T_3} \int_{-T_2}^{T_2} \int_{T_1}^{T_1+\zeta} \phi(q_1, q_2, q_3) dq_1 dq_2 dq_3 \\ - \int_{-T_3}^{T_3} \int_{-T_2}^{T_2} \int_{T_1-\zeta}^{T_1} \phi(q_1, q_2, q_3) dq_1 dq_2 dq_3 \\ - \int_{-T_3}^{T_3} \int_{-T_2}^{T_2} \int_{-T_1}^{-T_1+\zeta} \phi(q_1, q_2, q_3) dq_1 dq_2 dq_3 \\ + \int_{-T_3}^{T_3} \int_{-T_2}^{T_2} \int_{-T_1-\zeta}^{-T_1} \phi(q_1, q_2, q_3) dq_1 dq_2 dq_3 \end{bmatrix}$$

$$\left\{ A_k \right\}_{\text{any } k} \equiv \{A_1 \cup \dots \cup A_K\}$$

- for the detection test statistics (we modify the notation of equation (27) to include the absolute value):

$$q_k \equiv |\varepsilon_0 - \varepsilon_k| \quad (\text{A.23})$$

- for the exclusion test statistics:

$$q_{j,l} \equiv |\varepsilon_j - \varepsilon_{j,l}| \quad (\text{A.24})$$

where $\varepsilon_{j,l}$ is the subset solution that excludes both measurement subsets i and l

- whenever it is possible to keep the same notations, subscripts i , j and k are respectively used to designate indices of fault hypotheses, exclusion hypotheses, and detection test statistics.

APPENDIX III. INTEGRITY RISK EQUATION FOR SS RAIM FDE

First, the general integrity risk equation (38) is rewritten to distinguish hypotheses of:

- no detection under FF conditions
- no detection under faulty conditions
- detection and correct exclusion (CE)
- wrong exclusion (WE) under FF conditions
- wrong exclusion under faulty conditions

$$\begin{aligned} P_{HMI} &= P(HI, ND | H_0) P_{H_0} \\ &+ \sum_{i=1}^{n_H} P(HI, ND | H_i) P_{H_i} \\ &+ \sum_{i=1}^{n_H} P(HI, D, CE | H_i) P_{H_i} \\ &+ P(HI, D, WE | H_0) P_{H_0} \\ &+ \sum_{i=1}^{n_H} P(HI, D, WE | H_i) P_{H_i} \end{aligned} \quad (\text{A.22})$$

This appendix aims at establishing upper bounds on each of these groups of terms to enable practical integrity risk evaluation using protection level equations.

We use the following notations:

- for events A_k , $k=1, \dots, K$, we note:

$$\{A_k \forall k\} \equiv \{A_1, \dots, A_K\} = \{A_1 \cap \dots \cap A_K\}$$

Equation (A.22) can be reinterpreted using the four step SS exclusion procedure outlined in Section V. It follows that the first and second terms in equation (A.22) can be bounded as:

$$\begin{aligned} P(HI, ND | H_0) &= P(|\varepsilon_0| > \ell, q_k < T_k \forall k | H_0) \\ &\leq P(|\varepsilon_0| > \ell | H_0) \end{aligned} \quad (\text{A.25})$$

$$\begin{aligned} P(HI, ND | H_i) &= P(|\varepsilon_0| > \ell, q_k < T_k \forall k | H_i) \\ &\leq P(|\varepsilon_0| > \ell, q_i < T_i | H_i) \\ &\leq P(|\varepsilon_0| > \ell | H_i, q_i < T_i) P(q_i < T_i | H_i) \\ &\leq P(|\varepsilon_0| > \ell | H_i, q_i < T_i) \end{aligned} \quad (\text{A.26})$$

Equations (A.25) and (A.26) are integrity risk bounds corresponding to protection levels typically used in SS for detection only [2], [7]. It is worth noticing that no assumption needs be made on the correlation between ε_0 and q_i , so that these equations hold for estimators other than the least squares estimator.

Then, the next three terms account for the probability of hazardous information when excluding measurements:

$$\begin{aligned}
& P(HI, D, CE | H_i) \\
&= P \left(\begin{array}{l} |\varepsilon_i| > \ell, \mathbf{q}_k \underset{\text{any } k}{\geq} T_k, \\ \mathbf{q}_{j,l} < T_{j,l} \forall l \neq i | H_i \end{array} \right) \\
&\leq P(|\varepsilon_i| > \ell | H_i) = P(|\varepsilon_i| > \ell | H_0)
\end{aligned} \tag{A.27}$$

Since equation (A.27) captures the correct exclusion event, ε_i is fault-free. The distribution of ε_i under H_0 is known.

$$\begin{aligned}
& P(HI, D, WE | H_0) \\
&= \sum_{j=1}^{n_H} P \left(\begin{array}{l} |\varepsilon_j| > \ell, \mathbf{q}_k \underset{\text{any } k}{\geq} T_k, \\ \mathbf{q}_{j,l} < T_{j,l} \forall l \neq j | H_0 \end{array} \right) \\
&\leq \sum_{j=1}^{n_H} P(|\varepsilon_j| > \ell, \mathbf{q}_k \underset{\text{any } k}{\geq} T_k | H_0) \\
&\leq \min \left\{ \begin{array}{l} \sum_{j=1}^{n_H} P(|\varepsilon_j| > \ell | H_0), \\ \sum_{j=1}^{n_H} P(\mathbf{q}_k \underset{\text{any } k}{\geq} T_k | H_0) \end{array} \right\} \\
&\leq \min \left\{ \sum_{j=1}^{n_H} P(|\varepsilon_j| > \ell | H_0), n_H C_{REQD} \right\}
\end{aligned} \tag{A.28}$$

where C_{REQD} is the continuity risk allocation for detection ($C_{REQD} = \beta C_{REQ}$ in equation (47)). In (A.28), we have the option of picking two upper-bounds. We would like to keep the tightest bound to preserve availability. Because the bound in (A.28) is multiplied by P_{H0} in equation (A.22), and because it is unclear how large $P(|\varepsilon_j| > \ell | H_0)$ can become, we can choose not to disregard the second term bounded by $n_H C_{REQD}$, over which we have some control. This choice is application specific. The bound in $n_H C_{REQD}$ was not needed in the ARAIM performance evaluation of Section VI, and therefore it is not carried along in the main body of the paper.

$$\begin{aligned}
& P(HI, D, WE | H_i) \\
&= \sum_{\substack{j=1 \\ j \neq i}}^{n_H} P \left(\begin{array}{l} |\varepsilon_j| > \ell, \mathbf{q}_k \underset{\text{any } k}{\geq} T_k, \\ \mathbf{q}_{j,l} < T_{j,l} \forall l \neq j | H_i \end{array} \right) \\
&\leq \sum_{\substack{j=1 \\ j \neq i}}^{n_H} P(|\varepsilon_j| > \ell, \mathbf{q}_{j,l} < T_{j,l} \forall l \neq j | H_i) \\
&\leq \sum_{\substack{j=1 \\ j \neq i}}^{n_H} P(|\varepsilon_j| > \ell, \mathbf{q}_{j,i} < T_{j,i} | H_i) \\
&\leq \sum_{\substack{j=1 \\ j \neq i}}^{n_H} \left(P(|\varepsilon_j| > \ell | H_i, \mathbf{q}_{j,i} < T_{j,i}) \right. \\
&\quad \left. \times P(\mathbf{q}_{j,i} < T_{j,i} | H_i) \right) \\
&\leq \sum_{\substack{j=1 \\ j \neq i}}^{n_H} P(|\varepsilon_j| > \ell | H_i, \mathbf{q}_{j,i} < T_{j,i})
\end{aligned} \tag{A.29}$$

In the last step of (A.29), the distribution of ε_j under H_i is unknown, but its folded cumulative distribution function can be over-bounded using the condition ' $\mathbf{q}_{j,i} < T_{j,i}$ '.

Finally, we substitute the expressions for the SS test statistics in (A.23) and (A.24) into the integrity risk bounds (A. 25) to (A.29), and substitute the result back into (A.22). We can then make use of the conditions in equations (A.26) and (A.29) to bound the estimation error, after noticing that:

$$|\varepsilon_0| \leq |\varepsilon_i| + |\varepsilon_0 - \varepsilon_i| \quad \text{and} \quad |\varepsilon_j| \leq |\varepsilon_{j,l}| + |\varepsilon_j - \varepsilon_{j,l}| \tag{A.30}$$

We obtain a bound on P_{HMI} for which protection levels can be derived (as shown in equation (43)).

$$\begin{aligned}
P_{HMI} &\leq P(|\varepsilon_0| > \ell | H_0) P_{H0} \\
&\quad + \sum_{i=1}^{n_H} P(|\varepsilon_i| + T_i > \ell | H_i) P_{Hi} \\
&\quad + \sum_{i=1}^{n_H} P(|\varepsilon_i| > \ell | H_i) P_{Hi} \\
&\quad + \min \left(\sum_{j=1}^{n_H} P(|\varepsilon_j| > \ell | H_0), n_H C_{REQD} \right) P_{H0} \\
&\quad + \sum_{i=1}^{n_H} \sum_{\substack{j=1 \\ j \neq i}}^{n_H} P(|\varepsilon_{j,i}| + T_{j,i} > \ell | H_i) P_{Hi}
\end{aligned} \tag{A.31}$$

APPENDIX IV. CONTINUITY RISK EQUATION FOR SS RAIM FDE

First, the general continuity risk equation (39) is broken down to distinguish cases of no-exclusion under fault-free and fault hypotheses

$$P_{CONT} = P(D, NE | H_0)P_{H_0} + \sum_{i=1}^{n_H} P(D, NE | H_i)P_{H_i} \quad (A.32)$$

This appendix aims at establishing bounds on these two groups of terms. The same notations as in Appendix III are used. The first term in equation (A.32) can be bounded as follows:

$$\begin{aligned} P(D, NE | H_0) &= P(q_k \geq T_k, q_{j,l} \geq T_{j,l} \forall j | H_0) \\ &\leq P(q_k \geq T_k | H_0) \\ &\leq \sum_{k=1}^{n_H} P(q_k \geq T_k | H_0) \end{aligned} \quad (A.33)$$

This bound is similar to the one typically used in SS for detection only to limit the probability of false alarms. A second term is added when excluding measurements, which can be bounded in the following manner:

$$\begin{aligned} P(D, NE | H_i) &= P(q_k \geq T_k, q_{j,l} \geq T_{j,l} \forall j | H_i) \\ &\leq P(q_{j,l} \geq T_{j,l} \forall j | H_i) \\ &\leq P(q_{i,l} \geq T_{i,l} | H_i) = P(q_{i,l} \geq T_{i,l} | H_0) \\ &\leq \sum_{\substack{j=1 \\ j \neq i}}^{n_H} P(q_{i,j} \geq T_{i,j} | H_0) \end{aligned} \quad (A.34)$$

In equation (A.34), we obtain probability terms conditioned upon H_0 although the initial term is conditioned upon H_i . This is essential because the test statistic distribution under H_0 is known. This was achieved by isolating the test statistics that exclude the faulty measurement subset under H_i :

$$q_{i,l} \Big|_{any\ l \neq i} = |\varepsilon_i - \varepsilon_{i,l}| \quad (A.35)$$

Finally, substituting the expressions for the SS test statistics in (A.23) and (A.24) into the continuity risk

bounds (A.33) and (A.34), and substituting the result back into (A.32) provides the continuity risk bound of equation (45).

ACKNOWLEDGMENTS

We would like to thank the Federal Aviation Administration for sponsoring this work.

REFERENCES

- [1] Walter, T., Enge, P., Blanch, J., and Pervan, B., "Worldwide Vertical Guidance of Aircraft Based on Modernized GPS and New Integrity Augmentations," *Proc. of IEEE*, Vol. 96, No. 12, 2008.
- [2] Blanch, J., Walter, T., Enge, P., Wallner, S., Fernandez, F. A., Dellago, R., Ioannides, R., Hernandez, I. F., Belabbas, B., Spletter, A., Rippl, M., "Critical Elements for a Multi-Constellation Advanced RAIM", *NAVIGATION*, Vol. 60, No. 1, Spring 2013, pp. 53-69.
- [3] EU-US Cooperation on Satellite Navigation, WG C-ARAIM Technical Subgroup, "ARAIM Technical Subgroup Milestone 1 Report", 2012. available online : http://ec.europa.eu/enterprise/newsroom/cf/_getdocument.cfm?doc_id=7793
- [4] van Graas, F., Farrell, J., "Baseline Fault Detection and Exclusion Algorithm," *Proc. of the 49th Annual Meeting of The ION*, Cambridge, MA, June 1993, pp. 413-420.
- [5] Pervan, B., Lawrence, D., Cohen, C., and Parkinson, B., "Parity Space Methods for Autonomous Fault Detection and Exclusion Using GPS Carrier Phase," *Proceedings of IEEE Position Location and Navigation Symposium*, Atlanta, GA, 1996.
- [6] Blanch, J., Walter, T., Lee, Y., Pervan, B., Rippl, M., and Spletter, A., "Advanced RAIM User Algorithm Description: Integrity Support Message Processing, Fault Detection, Exclusion, and Protection Level Calculation," *Proc. of ION GNSS 2012*, Nashville, TN, Sept. 17-21, 2012, pp. 2828 - 2849.
- [7] Brenner, M., "Integrated GPS/Inertial Fault Detection Availability", *NAVIGATION*, Vol. 43, No. 2, Summer 1996, pp. 111-130.
- [8] Wang, J., and Ober, P., "On the Availability of Fault Detection and Exclusion in GNSS Receiver Autonomous Integrity Monitoring," *The Journal of Navigation of the Royal Institute of Navigation*, Vol. 62, 2009.
- [9] Joerger, M., Chan, F.-C., Langel, S., and Pervan, B., "RAIM Detector and Estimator Design to Minimize the Integrity Risk," *Proc. of ION GNSS 2012*, Nashville, TN, September 2012.
- [10] Potter, I. E., and Sunman, M. C., "Threshold-less Redundancy Management With Arrays of Skewed Instruments," *AGARDOGRAPH - No 224*, 1977, pp 15-11 to 15-25.

- [11] Sturza, M, "Navigation System Integrity Monitoring Using Redundant Measurements," *NAVIGATION: Journal of the Institute of Navigation*, Washington, DC, Vol. 35 No. 4, 1988, pp. 69-87.
- [12] Blanch, Juan, Ene, Alex, Walter, Todd, Enge, Per, "An Optimized Multiple Hypothesis RAIM Algorithm for Vertical Guidance," Proc. of ION GNSS 2007, Fort Worth, TX, September 2007, pp. 2924-2933.
- [13] Luenberger, D. G., and Ye, Y., *Linear and Nonlinear Programming – Third Edition*, Springer Editor, 2008.
- [14] Blanch, J., Walter, T., and Enge, P., "Results on the Optimal Detection Statistic for Integrity Monitoring," *Proc. of the 2013 International Technical Meeting of The ION*, San Diego, CA, January 2013, pp. 262-273.
- [15] Drezner, Z., and Wesolowsky, G. O., "On the Computation of the Bivariate Normal Integral." *Journal of Statistical Computation and Simulation*. Vol. 35, 1989, pp. 101–107.