THE JOURNAL OF NAVIGATION (2018), **71**, 1281–1298. © The Royal Institute of Navigation 2018
doi:10.1017/S0373463318000383

Fault Exclusion in Multi-Constellation Global Navigation Satellite Systems

Yawei Zhai[1], Mathieu Joerger[2] and Boris Pervan[1]

[1](*Illinois Institute of Technology*)
[2](*The University of Arizona*)
(E-mail: yzhai9@hawk.iit.edu)

This paper comprehensively investigates the fault exclusion problem in multi-constellation Global Navigation Satellite Systems (GNSS). In future GNSS, the heightened likelihood of fault detection events will cause more interruptions in the continuity of the navigation operation. The main contribution of this paper is to establish the theoretical basis to quantify the contributions of fault events on continuity risk, therefore allowing us to assess the desired exclusion function performance based on specific continuity requirements. Accordingly, a new real-time exclusion algorithm is developed, for which the upper bounds on integrity risks are rigorously derived. Using the new method, performance is comprehensively investigated for two important civil aircraft navigation operations using various numbers of constellations. We show that high service availability can be achieved for both operations.

KEYWORDS

1. Fault Exclusion. 2. Continuity. 3. Advanced Receiver Autonomous Integrity Monitoring (ARAIM).

Submitted: 2 December 2017. Accepted: 4 May 2018. First published online: 26 June 2018.

1. INTRODUCTION. The main challenge when using Global Navigation Satellite Systems (GNSS) in safety-critical civil aviation applications is to mitigate the integrity threats caused by measurement faults (Pervan, 1996). For the single constellation case, using the Global Positioning System (GPS) only, Fault Detection (FD) has been implemented using Receiver Autonomous Integrity Monitoring (RAIM) (Lee, 1986; Parkinson and Axelrad, 1988; RTCA Special Committee 159, 1991). The core principle of RAIM is to exploit redundant measurements to achieve self-contained FD at the user receiver (Joerger et al., 2014).

In the near term, four constellations including GPS (United States (US)), Globalnaya Navigatsionnaya Sputnikovaya Sistema (GLONASS) (Russia), Galileo (European Union (EU)) and BeiDou (China) are expected to finish their modernisations and/or full deployments (Gibbons, 2012), which will provide many more satellites in view than are available using GPS alone. This revolutionary development in GNSS, together with

https://doi.org/10.1017/S0373463318000383 Published online by Cambridge University Press

important advancements in the RAIM concept itself, will open the possibility to independently support all phases of aircraft navigation using GNSS. Therefore, considerable effort has recently been expended, especially in the EU and the US (Blanch et al., 2015; Federal Aviation Authority (FAA), 2010), to develop new dual-frequency, multi-constellation Advanced RAIM (ARAIM) Fault Detection and Exclusion (FDE) methods. Currently, two versions of ARAIM, corresponding to two operational scenarios, are being investigated. Horizontal ARAIM (H-ARAIM) aims at providing horizontal navigation integrity for aircraft en-route, terminal, initial approach, Non-Precision Approach (NPA) and departure operations. Vertical ARAIM (V-ARAIM) is intended for Localiser Performance with Vertical guidance (LPV) with the final goal of leading the aircraft to a 200-foot decision height, that is, LPV-200 (EU-US Cooperation on Satellite Navigation, 2016).

With multiple GNSS constellations available for future ARAIM, the impact of having a large number of available measurements on navigation performance is not entirely obvious. From the integrity perspective, we can naturally expect the conditional integrity risk under any given fault hypothesis to be reduced, but there is a chance that the accumulation of monitored fault modes increases the total (unconditioned) integrity risk. From the continuity perspective, because any reasonable FD algorithm will detect most faults, the accumulated likelihood of satellite and constellation faults with multiple constellations could dramatically increase ARAIM continuity risk. However, this impact has not been fully investigated in prior research. Even though the concept of fault exclusion has been introduced before (Blanch et al., 2014; 2016; Joerger et al., 2013; Joerger and Pervan, 2016), the algorithms are heuristic and not traceable to any specific navigation requirements. The key contribution of this paper is to establish the basis to quantify the contributions of fault events on continuity, which allows us to assess the desired exclusion function performance, or even the need of an exclusion function, based on specific continuity requirements.

In Section 2, we derive the equations to quantify the contributions of fault events on ARAIM continuity, based on the navigation requirements for intended ARAIM operations. The relationships among the failure rates, the GNSS ground segment Mean Time To Notify (MTTN) the users, and the exposure times are rigorously derived. In particular, when computing the V-ARAIM continuity risk, to accommodate the requirement, we show that a conversion is required for fault prior probabilities. To achieve this, the assumptions are laid out and the rationale is clarified.

Section 3 describes the method to assess the need for airborne exclusion, and the process to establish the requirements for the exclusion function itself. Given the nominal ARAIM fault probabilities (Walter et al., 2016) and the continuity risk equations developed in Section 2, it will be shown that, for dual-constellation V-ARAIM, the accumulated probability of fault occurrence is below the allocated continuity requirement, which means that an exclusion function does not need to be implemented. However, when more constellations are used, or the constellations are subject to larger fault probabilities, exclusion may be required; these cases are specifically identified. For H-ARAIM, we show that the continuity requirement is much more stringent, so airborne exclusion is always required to improve continuity.

Section 4 presents the fault exclusion scheme by describing the real-time ARAIM exclusion algorithm: deriving the equations to compute the exclusion thresholds and bound the associated FDE integrity risk. A Solution Separation (SS) exclusion algorithm is designed, and the practical implementation procedures are detailed. To evaluate the integrity risk for

https://doi.org/10.1017/S0373463318000383 Published online by Cambridge University Press

Table 1. Navigation requirements of RNP 0·1 and LPV-200.

	Vertical Alert Limit (VAL)	Horizontal Alert Limit (HAL)	Integrity Risk Requirement	Continuity Risk Requirement
RNP 0·1	N/A	185 m (0·1 nm)	10^{-7}/hour	10^{-8}/hour to 10^{-4}/hour
LPV-200	35 m	40 m	10^{-7}/approach	8×10^{-6}/15 sec

the FDE algorithm, a conservative but computationally efficient upper bound is derived. This algorithm is based on the previous work in Zhai et al. (2016) and Joerger and Pervan (2016).

With the theoretical methods fully characterised, Section 5 quantifies the achievable ARAIM performance over various numbers of constellations. To investigate the impact of the increased measurement redundancy on integrity and continuity, two separate analyses are carried out: (a) V-ARAIM availability with FD function only and (b) overall ARAIM performance with both detection and exclusion functions. The results of (a) show that adding more measurements into the system could significantly improve navigation integrity. In regard to the second analysis, (b), both the integrity and continuity requirements are considered. By implementing the new exclusion scheme, high availability performance can be provided by both V- and H-ARAIM.

2. QUANTIFYING CONTINUITY RISK.

This section addresses the impact of GNSS faults on ARAIM continuity and develops the basis to quantify their contributions to continuity risk, based on the navigation requirements listed in Table 1 (International Civil Aviation Organization (ICAO), 2009; FAA, 2012). Required Navigation Performance (RNP) 0·1 and LPV-200, which correspond to the most stringent navigation requirements for H- and V-ARAIM (EU-US Cooperation on Satellite Navigation, 2016), are employed throughout this paper as vehicles to quantify the ARAIM performance.

The V-ARAIM continuity risk requirement $C_{REQ,V}$ is specified as 8×10^{-6} per 15 seconds. According to ICAO, this requirement applies to average risk (over time) of Loss Of Continuity (LOC), and is normalised to a 15-second exposure time (ICAO, 2009). For the H-ARAIM continuity risk requirement $C_{REQ,H}$, the existence of a range, rather than a single value, accounts for the impact of the number of aircraft using the same service in the same area. For example, the intermediate value 10^{-6}/hour can be used for the situations of high air traffic density and airspace complexity, but the means to mitigate the LOC impact are present (ICAO, 2009). Since civilian commercial aircraft have a mandatory requirement for a backup navigation method, we choose $C_{REQ,H} = 10^{-6}$/hour for simulation purposes in this research.

Obviously, to properly evaluate the overall continuity risk, or probability of LOC (P_{LOC}), all the sources that cause LOC must be properly accounted for. However, because ARAIM continuity has been paid less attention than integrity in the literature, False Alarm (FA) is the only LOC source that has been considered to date (Blanch et al., 2010; Lee and McLaughlin, 2007). In reality, there are many other possible causes of LOC, including FD, unscheduled satellite outages, ionospheric scintillation, and radio frequency interference (EU-US Cooperation on Satellite Navigation, 2016; Zhai et al., 2017). In particular, given the large number of GNSS measurements and the different failure rates between constellations, multi-constellation ARAIM continuity can be severely affected by frequent FD.

https://doi.org/10.1017/S0373463318000383 Published online by Cambridge University Press

Therefore, FA and FD are considered as two main continuity threats in this paper. We will assign a continuity budget to account for the other events and assume their continuity risk contributions are always below the budget.

To quantify the P_{LOC} contribution from FD, the mechanisms to describe the ARAIM failure model must be clarified. Current work on defining the fault model is based on GPS commitments and historical data (Walter et al., 2016). Since other Constellation Service Providers (CSP) have not clearly established the fault descriptions for their constellations, this paper employs GPS as the representative. GPS Standard Positioning Service (SPS) Performance Standard (PS) commits to the single satellite failure rate R_{sat} of 10^{-5}/hour, which corresponds to having fewer than three Space Vehicle (SV) faults per year (US Department of Defense (DOD), 2008). Assuming an MTTN of 1 hour, which is conservatively representative of current GPS performance, the single satellite fault state probability P_{sat} at any time is 10^{-5} (Heng et al., 2012). Therefore, unless otherwise specified, we will use 10^{-5} for a single SV fault mode in this paper. As for the constellation faults, even though the GPS CSP is expected to commit to a constellation fault prior probability P_{const} of 10^{-6} in the future SPS PS, we stay consistent with current ARAIM fault assertions at this stage. Based on Walter et al. (2016), the following P_{const} values are respectively applied:

- V-ARAIM: 10^{-4} for all constellations;
- H-ARAIM: 10^{-8} for GPS, 10^{-4} for other constellations.

Note that these P_{sat} and P_{const} values are employed here just for demonstration purposes, and they may change in the future.

2.1. *H-ARAIM continuity risk.* Equation (1) shows the overall H-ARAIM continuity risk $P_{LOC,H}$ when only a detection function is implemented (that is, without exclusion capability). The probabilities of FA and FD are respectively expressed as $P_{FA,H}$ and $P_{FD,H}$, and all other LOC sources are grouped in $P_{other,H}$.

$$P_{LOC,H} = P_{FA,H} + P_{FD,H} + P_{other,H} \tag{1}$$

where

$$P_{FA,H} = P(D_0|H_0)P_{H_0} \quad \text{and} \quad P_{FD,H} = \sum_{i=1}^{N} P(D_0|H_i)P_{H_i} \tag{2}$$

D_0 represents the detection event using all satellites in view, H_i denotes the i-th fault mode, N is the total number of fault modes, and H_0 represents the Fault-Free (FF) state. As described in Blanch et al. (2015), the prior probabilities P_{H_i} can be evaluated using P_{sat} and P_{const}.

2.2. *V-ARAIM Continuity Risk.* Similar to Equation (1), the total V-ARAIM continuity risk $P_{LOC,V}$ with only a detection function, is expressed as Equation (3).

$$P_{LOC,V} = m(P_{FA,V} + P_{FD,V}) + P_{other,V} \tag{3}$$

When two runways are closely-spaced, the V-ARAIM continuity requirement needs to be adjusted (ICAO, 2009). This is because the navigation service can be used by many aircraft at the same time, and they may simultaneously lose continuity due to common system failure. If two runways are closely-spaced and are handled by the same Air Traffic Controller (ATC), the simultaneous missed approaches will result in increased stress for

https://doi.org/10.1017/S0373463318000383 Published online by Cambridge University Press

Table 2. V-ARAIM continuity budget allocation.

$P_{FF,V,REQ}$	$P_{FP,V,REQ}$	$P_{other,V,REQ}$
2×10^{-6}/15 sec	5×10^{-6}/15 sec	10^{-6}/15 sec

the ATC. Therefore, to address the impact of the navigation interruptions on more than one aircraft approach, the multiplier m is introduced in Equation (3), and $m = 2$ is assumed in this paper. However, it is worth clarifying that the purpose of introducing this multiplier is to make the equation general and rigorous. Operationally, such a case may rarely happen so m can be set to be 1 most of the time. The choice in this paper is to capture the worst-case operational scenario.

$$P_{FA,V} = P(D_0|H_0)\lambda P_{H_0} \quad \text{and} \quad P_{FD,V} = \sum_{i=1}^{N} \gamma P(D_0|H_i)\lambda P_{H_i}, \text{ where } \lambda = \frac{15 \text{ sec}}{1 \text{ hour}} \tag{4}$$

To accommodate $C_{REQ,V}$, the fault probabilities P_{H_i} need to be scaled to a 15-second exposure interval (Zhai et al., 2015). Unlike integrity risk, which is affected by latent faults, LOC occurs only at the transition moment from continuous service to sudden interruption. Let us assume all the faults can be detected, and detection always occurs during an approach. Even though a fault may last an hour or more before it is identified by the ground segment, if it does not impact the aircraft anymore once detected, one fault will cause only one LOC in one 15 second segment, regardless of when the fault is detected. Therefore, the multiplier λ in Equation (4) is applied to convert the fault probability P_{H_i} into the 15-second interval.

In the justification above, it is implicitly assumed that a fault does not cause more than one missed approach for the same aircraft. However, despite the small likelihood, this situation may happen when (a) the aircraft is exposed to a long-lasting fault, (b) a second approach is attempted following a missed approach due to FD, and (c) the fault is not detected again prior to the second approach but is detected again during the second approach. To account for such a scenario, the multiplier γ is introduced in Equation (4). Assuming one tenth of aircraft may be exposed to the same fault again during their second approach, $\gamma = 1{\cdot}1$ is employed in this paper.

3. NEED AND REQUIREMENTS FOR ARAIM EXCLUSION.

Using the relationships established in Section 2, in this section we will comprehensively assess the need of exclusion over multiple criteria, identify the cases when the exclusion function is required, and derive the associated requirements for the exclusion function.

3.1. *Need for V-ARAIM exclusion for continuity.*

To respectively limit each LOC contribution, the overall continuity risk requirement $C_{REQ,V}$ is allocated to the different sources. Table 2 lists an example allocation that will be used throughout the remainder of this paper. The three components in the first row correspond to a LOC event under the FF condition, the Fault-Present (FP) condition and all other causes.

To examine the need for the V-ARAIM exclusion function, the FD probability under the FP condition should be computed. To do this, we use the first two terms in Equation (5) below. The rightmost term in Equation (5) is a tight bound on this probability, because the likelihood of detecting a fault under these conditions will be very close to one by design. If

https://doi.org/10.1017/S0373463318000383 Published online by Cambridge University Press

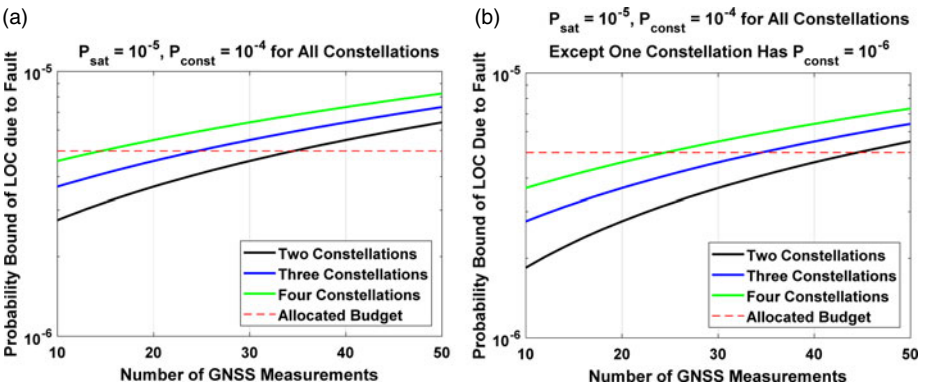


Figure 1. Probability bound of LOC due to fault with varying numbers of measurements.

it turns out that the bound is smaller than $P_{FP,V,REQ}$, then a V-ARAIM exclusion function is not required for continuity.

$$mP_{FD,V} = m\sum_{i=1}^{N}\gamma P(D_0|H_i)\lambda P_{H_i} < m\gamma\sum_{i=1}^{N}\lambda P_{H_i} \tag{5}$$

As revealed by Equation (5), the value of the bound is most directly influenced by the fault mode prior probabilities and the total number of fault modes, N. The latter, in turn, is dependent on the number of constellations and satellites used, because N accounts for all the faulty SV combinations including single satellite fault, multiple satellite fault and constellation fault. Whether a V-ARAIM exclusion function is needed or not could vary over different operational scenarios. We investigate multiple representative cases using two, three and four constellations, for which $m = 2$ and $\gamma = 1{\cdot}1$ are applied. The sensitivity analyses are achieved by varying the number of measurements and the values of P_{sat} and P_{const}.

Figure 1 illustrates the probability bound of Equation (5) as a function of the average number of visible satellites. In each figure, three solid lines correspond to the number of constellations being investigated, and the red dashed line is the allocated continuity budget $P_{FP,V,REQ}$. Therefore, an exclusion function is not required when the solid lines are below the red lines. Under the dual-constellation scenario in Figure 1(a), the intersection between the black line and the threshold occurs when the average number of satellites is more than 35. It is highly unlikely that this number will ever be reached with any two constellations, which implies an airborne exclusion function is not needed using dual-constellation V-ARAIM. For the four-constellation scenario in Figure 1(a), the green line is above the threshold if the average number of SVs exceeds 15. In this case, with four constellations, it is quite likely that the average number of visible satellites will far exceed 15 visible SVs using four constellations, so the heightened continuity risk will need to be reduced by an exclusion function.

Figure 2 shows the tolerable P_{sat} and P_{const} values for one constellation to meet the allocated continuity budget, while assuming all other constellations are subject to nominal fault probabilities, that is, $P_{sat} = 10^{-5}$ and $P_{const} = 10^{-4}$. The three lines in each figure define the borders of whether or not implementing the exclusion function is required. An exclusion

https://doi.org/10.1017/S0373463318000383 Published online by Cambridge University Press

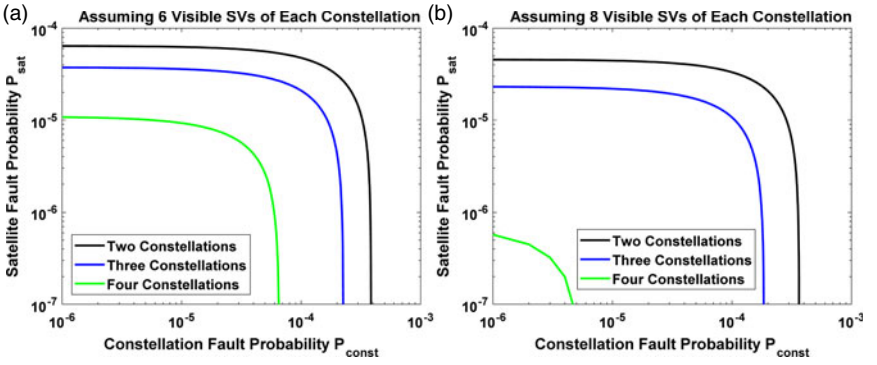


Figure 2. P_{sat} vs. P_{const} for one constellation to meet the allocated continuity requirement.

function is not needed if the values of P_{sat} and P_{const} are located in the region under and to the left of the solid lines. The results show that, in all cases, a V-ARAIM exclusion function would be required for continuity if any one of the constellations is subject to P_{sat} of 10^{-4}, or P_{const} of 10^{-3}.

3.2. *Requirements for V-ARAIM Exclusion.* With an exclusion function implemented, only those detection events that the exclusion function cannot resolve would result in a LOC. These can be further separated into two classes: (1) under FF conditions, a FA can be followed by No Exclusion (FANE), and (2) a FD can be followed by (FDNE). The V-ARAIM FDE functions must be defined to limit these two events.

The probability of FANE can be quantified and bounded by the following equation:

$$mP_{FANE,V} = mP(D_0, \bar{E}_0|H_0)\lambda P_{H_0} < mP(D_0|H_0)\lambda P_{H_0} \tag{6}$$

where $\bar{E}_0$ denotes the event that no exclusion can be made using all satellites in view. The upper bound of Equation (6) is the FA event, so the LOC contribution to V-ARAIM FANE can be controlled by setting detection thresholds. When a fault is present, the probability of LOC is:

$$mP_{FDNE,V} = m\sum_{i=1}^{N}\gamma P(D_0, \bar{E}_0|H_i)\lambda P_{H_i} < m\sum_{i=1}^{N}\gamma P(\bar{E}_0|H_i)\lambda P_{H_i} \tag{7}$$

Limiting the bound in Equation (7) to meet $P_{FP,V,REQ}$ can be achieved by appropriately setting exclusion thresholds. The ARAIM FDE tests will be introduced in the next section.

It must be clarified that to generate the quantitative results in Section 3.1, we chose an example continuity requirement allocation and example scale factors. Because we seek to build a general method that rigorously accounts for all possible LOC contributions, conservative values were selected. Therefore, the conclusion from those example analyses may not be suitable for all operational conditions. For instance, it is not always necessary to use $m = 2$, especially for airports with widely dispersed runways. In addition, less conservative fault probabilities—for example, based on historical data—may be used when computing continuity risk. Such changes could reduce the FD probability, and may potentially lead to the conclusion that exclusion is not required for V-ARAIM even if three or four constellations are used. Further, even though we use conservative values, the green line in Figure 1(a) shows the total LOC probability bound exceeds the requirement (8×10^{-6}) by only a small amount, which might be acceptable from an operational perspective. For this

https://doi.org/10.1017/S0373463318000383 Published online by Cambridge University Press

Table 3. H-ARAIM continuity budget allocation.

$P_{FF,H,REQ}$	$P_{FP,H,REQ}$	$P_{other,H,REQ}$
4×10^{-7}/hour	4×10^{-7}/hour	2×10^{-7}/hour

reason, in the later sections of this paper, V-ARAIM performance is investigated separately using the FD-only function and the FDE function.

3.3. *Requirement for H-ARAIM exclusion.* Table 3 lists the H-ARAIM continuity requirement allocation among FF condition, FP condition, and all other sources. The need for H-ARAIM exclusion can be assessed using the same approach as for V-ARAIM. Given the stringent value of $C_{REQ,H}$, the conclusion appears obvious; even the single satellite fault rate for GPS (10^{-5}/hr) already dramatically exceeds the requirement. Therefore, an H-ARAIM exclusion function must be implemented to improve continuity.

In this case, the overall H-ARAIM LOC probability is given by Equation (8). Equations (9) and (10) express the bounds on the FANE and FDNE contributions, which should be respectively limited to be smaller than $P_{FF,H,REQ}$ and $P_{FP,H,REQ}$ in Table 3.

$$P_{LOC,H} = P_{FANE,H} + P_{FDNE,H} + P_{other,H} \tag{8}$$

$$P_{FANE,H} = P(D_0, \bar{E}_0|H_0)P_{H_0} < P(D_0|H_0)P_{H_0} \tag{9}$$

$$P_{FDNE,H} = \sum_{i=1}^{N} P(D_0, \bar{E}_0|H_i)P_{H_i} < \sum_{i=1}^{N} P(\bar{E}_0|H_i)P_{H_i} \tag{10}$$

4. FAULT EXCLUSION SCHEME. In this section, we present a detailed, step-by-step description of a new SS-based exclusion algorithm and derive the associated FDE integrity risk bound. This algorithm is primarily intended to serve as an exclusion function for H-ARAIM, but it can also be directly applied to improve V-ARAIM continuity when needed.

4.1. *Real-time FDE algorithm.* The 'real-time' algorithm refers to the processes implemented at the airborne user receiver. As shown in Figure 3, the algorithm starts with evaluating the instantaneous integrity risk P_{HMI} or Protection Level (PL) of the current geometry. For continuity, the key design element is the follow-up exclusion step after detection, and the mechanism to determine which SV(s) to exclude, both of which will be described.

The baseline Multiple Hypotheses SS (MHSS) ARAIM detection algorithm has been well defined and clarified (Joerger et al., 2014; Blanch, et al., 2015; EU-US Cooperation on Satellite Navigation, 2016). Using similar notations as our previous work (Zhai et al., 2016), the normalised detection test statistics q_d can be expressed as:

$$q_d = \frac{\hat{x}_0 - \hat{x}_d}{\sigma_{\Delta_d}} = \frac{\varepsilon_0 - \varepsilon_d}{\sigma_{\Delta_d}}, \quad \text{for } d = 1, \ldots, n \tag{11}$$

where $\hat{x}_0$ is the least squares position estimate using all-in-view satellites; $\hat{x}_d$ is the least squares position estimate using all in-view satellites except the ones included in fault mode $d, d = 1, \ldots, n$; n is the number of all fault modes that need to be monitored; σ_{Δ_d} is the standard deviation of the SS detection statistic Δ_d, which is defined as the difference between $\hat{x}_0$ and $\hat{x}_d$; ε_0 is the position estimate error of $\hat{x}_0$, having a normal distribution with bias of

https://doi.org/10.1017/S0373463318000383 Published online by Cambridge University Press

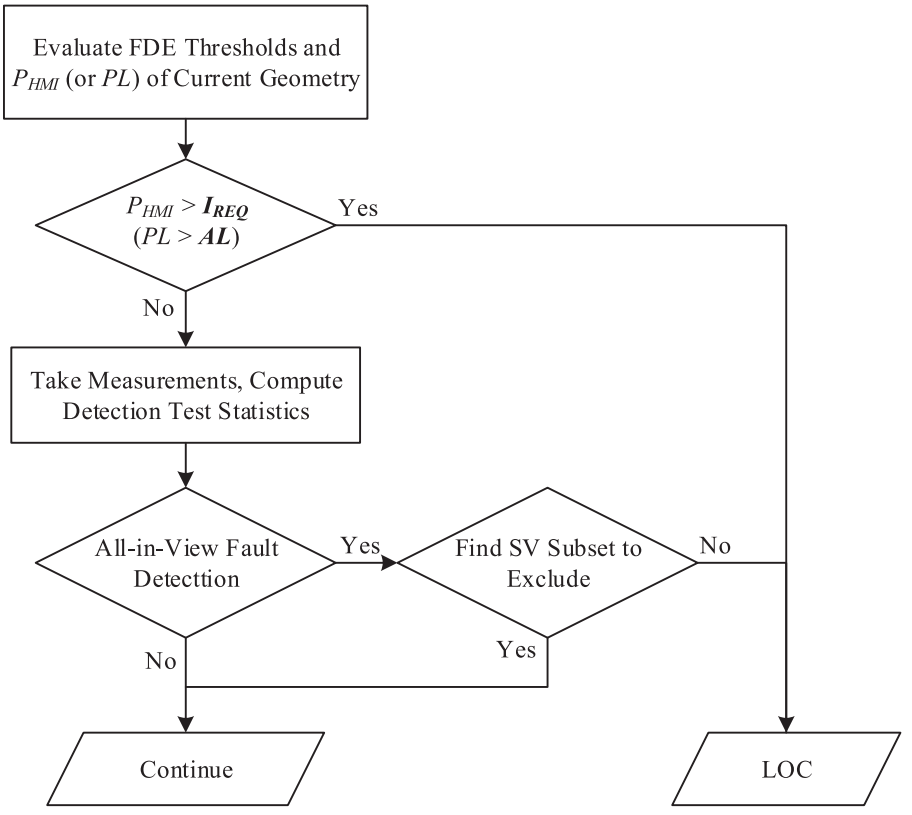


Figure 3. Flow diagram of the FDE algorithm.

b_0 and standard deviation σ_0 and ε_d is the position estimate error of $\hat{x}_d$, having a normal distribution with bias of b_d and standard deviation σ_d.

In the detection step, all the statistics in Equation (11) are evaluated and compared with their corresponding detection thresholds T_d, which are predefined based on the allocated FA requirement. If any of the statistics exceed the threshold, an alarm is issued, which indicates a fault exists in the system. Otherwise, if all the test statistics are smaller than their corresponding thresholds, there is no detection event and the operation continues.

Once an alarm occurs, the exclusion function will be executed. In this design, the exclusion function is composed of a two-step process. The first step determines the exclusion option order by arraying all q_d in a magnitude descending sequence. The first exclusion option corresponds to the fault mode with maximum statistic. The principle behind formatting in this order is due to the distributions of SS detection statistics. As the statistics are the differences between the all-in-view and satellite subset solutions in the position domain; under a faulted condition, it is most likely that the one corresponding to the actual fault is much larger than the others. It is worth mentioning that the purpose of the first step is to provide an efficient route for the algorithm to quickly make the final exclusion decision. There are cases when the actual fault mode does not result in the maximum statistic, especially when the constellation is exposed to more than one SV failure. That is why the second step has to be applied.

https://doi.org/10.1017/S0373463318000383 Published online by Cambridge University Press

In the second step, the final exclusion option is determined. It employs a second layer detection test to confirm there is no alarm in the satellite subset. The normalised exclusion statistics $q_{e,k}$ (or second layer detection statistics) are defined as:

$$q_{e,k} = \frac{\hat{x}_e - \hat{x}_{e,k}}{\sigma_{\Delta_{e,k}}} = \frac{\varepsilon_e - \varepsilon_{e,k}}{\sigma_{\Delta_{e,k}}}, \quad \text{for } k = 1, \ldots, n_e. \tag{12}$$

where $\hat{x}_{e,k}$ is the least squares position estimate using the remaining satellites after excluding fault mode $e, e = 1, \ldots, n$, except the ones in the second layer fault mode $k, k = 1, \ldots, n_e$; $\sigma_{\Delta_{e,k}}$ is the standard deviation of the exclusion statistic $\Delta_{e,k}$, which is defined as the difference between $\hat{x}_e$ and $\hat{x}_{e,k}$ and $\varepsilon_{e,k}$ is the position estimate error of $\hat{x}_{e,k}$, having a normal distribution with bias $b_{e,k}$ and standard deviation $\sigma_{e,k}$.

This step goes through all the exclusion options following the order determined in step 1. For each option, the exclusion test compares each $q_{e,k}$ with its associated exclusion threshold $T_{e,k}$, which is determined by the continuity requirement. If all the exclusion statistics are within their thresholds, then the associated satellite(s) in the candidate fault mode is/are chosen to be excluded. However, it is possible that no exclusion can be made even after testing all the options. This case will result in a LOC, and its probability of occurrence has been captured in Equations (7) and (10). In summary, two conditions will result in a satellite subset j being excluded (E_j): (a) there is no second layer detection after excluding this subset ($\bar{D}_j$) or (b) this subset corresponds to the maximum detection statistic among the subsets that pass the exclusion test (MAX_j).

4.2. *Evaluating FDE thresholds.* With the FDE algorithm specified, the events of fault detection (D_0) and no exclusion ($\bar{E}_j$) can be expressed in mathematical terms. The detection and exclusion thresholds for H-ARAIM can be computed respectively using the following equations:

$$T_d = Q^{-1}\left\{\frac{P_{FF,H,REQ}}{2P_{H_0} \cdot n}\right\} \tag{13}$$

$$T_{i,k} = Q^{-1}\left\{\frac{P_{FP,H,REQ,Hi}}{2 \cdot n_e}\right\}, \quad \text{where } P_{FP,H,REQ,Hi} = \frac{P_{FP,H,REQ}}{n \cdot P_{H_i}} \tag{14}$$

where $Q^{-1}(\cdot)$ is the inverse tail probability function of the standard normal distribution. Equations (13) and (14) are derived in the Appendix, based on the H-ARAIM continuity requirement. For V-ARAIM, if exclusion is implemented, these two equations can also be applied. A minor modification may be needed to accommodate the multipliers in Equations (6) and (7).

4.3. *Quantifying FDE integrity risk.* Since the *a priori* integrity risk evaluation is adopted as shown in Figure 3, when computing the instantaneous P_{HMI}/PL in real-time, the receiver does not know whether there is a fault detection or not, and which satellite subset needs to be excluded. Therefore, all possible situations that cause integrity threats need to be characterised. As a result, the instantaneous P_{HMI}/PL are identical to the predictive P_{HMI}/PL, which are usually evaluated for offline analyses purposes, and both need to account for the risks introduced by the exclusion options (Joerger and Pervan, 2016):

$$P_{HMI} = P(HI_0, \bar{D}_0) + \sum_{j=1}^{n} P(HI_j, E_j, D_0) \tag{15}$$

https://doi.org/10.1017/S0373463318000383 Published online by Cambridge University Press

In Equation (15), HI_0 and HI_j respectively represent the events that hazardous information exists in (a) a full-set position solution and in (b) a subset solution after excluding satellite(s) in fault mode j. $\bar{D}_0$ denotes a no fault detection event using all-in-view satellites. It can be bounded by employing the multiple fault hypothesis approach:

$$P_{HMI} < \sum_{i=0}^{n} \max_{f_i} \left(P(HI_0, \bar{D}_0 | H_i, f_i) + \sum_{j=1}^{n} P(HI_j, \bar{D}_j, MAX_j, D_0 | H_i, f_i) \right) P_{H_i} + P_{NM} \quad (16)$$

where P_{NM} denotes the summation of prior probabilities for all non-monitored fault modes (Blanch et al., 2015). There is an expansion of notation from Equation (15) to (16), where the exclusion event E_j in the former is decomposed in terms of both $\bar{D}_j$ and MAX_j. Under the hypothesis H_i, the actual fault vector is f_i, which can be fully described by its direction and magnitude (Joerger et al., 2014). The worst-case fault is obtained when the conditional FDE integrity risk for H_i (the summation over all exclusion options under hypothesis H_i) is maximised. However, directly evaluating P_{HMI} using Equation (16) is almost impossible because (a) searching for the worst-case fault over all exclusion options is an arduous task, especially when H_i is a multiple-satellite fault mode, and (b) the correlations between the events in each exclusion option are complex. In response, we seek a more computationally efficient upper bound.

$$P_{HMI} - P_{NM} < \sum_{i=0}^{n} P\left(HI_0, \bar{D}_0 | H_i\right) P_{H_i} + \sum_{i=0}^{n} \sum_{j=1}^{n} P\left(HI_j, \bar{D}_j, MAX_j, D_0 | H_i\right) P_{H_i} \quad (17)$$

In Equation (17), we have implicitly selected f_i to maximise each term individually. In contrast, in Equation (16), a single fault mode is selected to maximise the sum of all the terms. Therefore, summing the maximised individual risks using Equation (17) always bounds the maximised summed risk in Equation (16).

The first summation term on the right side of Equation (17) corresponds to the detection-only integrity risk, $P_{HMI,FD,only}$, for which the bounding methods have already been well established in several prior works. Here, we take advantage of the results in Joerger et al. (2014) and Blanch et al. (2015), and directly use the following upper bound of Equation (20) for this term:

$$P_{HMI,FD,only} = P\left(HI_0, \bar{D}_0 | H_0\right) P_{H_0} + \sum_{i=1}^{n} P\left(HI_0, \bar{D}_0 | H_i\right) P_{H_i} \quad (18)$$

$$< P\left(|\varepsilon_0| > \ell | H_0\right) P_{H_0} + \sum_{i=1}^{n} P\left(|\varepsilon_0| > \ell, \bigcap_{d=1}^{n} |q_d| < T_d | H_i\right) P_{H_i} \quad (19)$$

$$< P\left(|\varepsilon_0| > \ell | H_0\right) P_{H_0} + \sum_{i=1}^{n} P\left(|\varepsilon_i| + \sigma_{\Delta_i} T_i > \ell | H_i\right) P_{H_i} \quad (20)$$

where ℓ is the alert limit (AL). Equation (20) will be used to compute the P_{HMI} (or PL) if only the FD function is implemented.

Our attention is now turned to the second (double summation) term on the right side of Equation (17), which carries the cost of increased integrity risk by implementing exclusion.

https://doi.org/10.1017/S0373463318000383 Published online by Cambridge University Press

We first define $P_{HMI,i,j}$ as the integrity risk contribution after excluding E_j under hypothesis H_i. For the FF condition, H_0, since the position estimation error ε_j is expected to be significantly smaller than AL, $P_{HMI,0,j}$ can still be tightly bounded by eliminating all other information:

$$P_{HMI,0,j} = P\left(HI_j, \bar{D}_j, MAX_j, D_0 | H_i\right) P_{H_0} \tag{21}$$

$$< P\left(HI_j | H_0\right) P_{H_0} = P\left(\left|\varepsilon_j\right| > \ell \ | H_0\right) P_{H_0} \tag{22}$$

For the other fault hypotheses H_i, the exclusion events can be classified into two categories: Correct Exclusion (CE) and Wrong Exclusion (WE). Equation (22) can also be applied to tightly bound the integrity risk of a CE event, because if the actual faulted satellite subset S_i belongs to the excluded subset S_j, the post-exclusion position estimate $\hat{x}_j$ is also FF. In regard to the WE event, we employ the following bounding steps, leading to a final upper bound of Equation (26) that can be evaluated with great computational efficiency.

$$P_{\substack{HMI,i,j \\ S_i \not\subset S_j}} = P\left(HI_j, \bar{D}_j, MAX_j, D_0 | H_i\right) P_{H_i} \tag{23}$$

$$< P\left(HI_j, \bar{D}_j | H_i\right) P_{H_i} = P\left(|\varepsilon_j| > \ell, \bigcap_{k=1}^{n_e} |q_{j,k}| < T_{j,k} | H_i\right) P_{H_i} \tag{24}$$

$$< P\left(|\varepsilon_j| > \ell, |q_{j,i}| < T_{j,i} | H_i\right) P_{H_i} \tag{25}$$

$$< P\left(|\varepsilon_{j,i}| + \sigma_{\Delta_{j,i}} T_{j,i} > \ell | H_i\right) P_{H_i} \tag{26}$$

To improve computational efficiency, the knowledge of MAX_j and D_0 is eliminated in the progression from Equation (23) to (24), which implies the exclusion option order does not impact the final integrity risk upper bound (Milner et al., 2017). This is consistent with the original motivation of designating the order, which aims to speed up the real-time exclusion decision-making process, and is not aimed at improving integrity. In summary, the overall FDE integrity risk associated with the proposed algorithm can be upper-bounded and evaluated by substituting Equations (20), (22) and (26) into Equation (27) (Joerger and Pervan, 2016):

$$\begin{aligned} P_{HMI} - P_{NM} < & P\left(|\varepsilon_0| > \ell | H_0\right) P_{H_0} + \sum_{i=1}^{n} P\left(|\varepsilon_i| + \sigma_{\Delta_i} T_i > \ell | H_i\right) P_{H_i} \\ & + \sum_{j=1}^{n} \begin{pmatrix} P\left(|\varepsilon_j| > \ell | H_0\right) P_{H_0} + \sum_{\substack{i=1 \\ S_i \subset S_j}}^{n} P\left(|\varepsilon_j| > \ell | H_i\right) P_{H_i} \\ + \sum_{\substack{i=1 \\ S_i \not\subset S_j}}^{n} P\left(|\varepsilon_{j,i}| + \sigma_{\Delta_{j,i}} T_{j,i} > \ell | H_i\right) P_{H_i} \end{pmatrix} \end{aligned} \tag{27}$$

The PL is an alternative way to express the information contained in the FDE integrity risk bound Equation (27). The PL is a more practical metric in many cases (Blanch, et al., 2010; 2015), especially when the ALs of the operations are unknown. The PL corresponding to Equation (27) can be computed (iteratively) using Equation (28). The derivation of Equation (28) can be found in Appendix D of Cassel (2017), and a method to solve the

https://doi.org/10.1017/S0373463318000383 Published online by Cambridge University Press

Table 4. Multi-constellation ARAIM simulation parameters.

Constellation	24GPS + 24Galileo + 23GLONASS + 27Beidou
Mask Angle	5 degrees
User Grid	Latitude by Longitude: 10deg × 10deg
Simulation Time Period	1 day
Time Steps	10 mins
Error Model	Nominal Model Described in (EU-US Cooperation on Satellite Navigation, 2016)
Coverage Range	V-ARAIM: −70deg to 70deg latitude H-ARAIM: worldwide
P_{sat}	10^{-5}
P_{const}	V-ARAIM: 10^{-4} for all constellations H-ARAIM: 10^{-8} for GPS, 10^{-4} for others
σ_{URA}	V-ARAIM: 1m, H-ARAIM: 2·4m
σ_{URE}	$2/3\sigma_{URA}$
b_{nom}	0·75m

equation is introduced in Appendix E of the same document.

$$I_{REQ} - P_{NM} < 2Q\left(\frac{PL - b_0}{\sigma_0}\right) + \sum_{i=1}^{n} Q\left(\frac{PL - b_i - \sigma_{\Delta_i} T_i}{\sigma_i}\right) P_{H_i} + \sum_{j=1}^{n}\left(2Q\left(\frac{PL - b_j}{\sigma_j}\right) + \sum_{\substack{i=1 \\ S_i \not\subset S_j}}^{n} Q\left(\frac{PL - b_{j,i} - \sigma_{\Delta_{j,i}} T_{j,i}}{\sigma_{j,i}}\right) P_{H_i}\right) \quad (28)$$

5. MULTI-CONSTELLATION ARAIM PERFORMANCE. With the theoretical methods being derived in previous sections, this section investigates multi-constellation ARAIM navigation performance, and addresses the impact of increased numbers of measurements on integrity and continuity. Because an exclusion function must be implemented to improve H-ARAIM continuity, and whether or not exclusion function is needed for V-ARAIM largely depends on the operational scenario, we respectively analyse performance (a) using FD function only for V-ARAIM, and (b) applying both detection and exclusion functions for four-constellation V-ARAIM and dual-constellation H-ARAIM.

The analyses are performed under the baseline simulation conditions (EU-US Cooperation on Satellite Navigation, 2016), which are listed here in Table 4. It is important to note that the ARAIM navigation performance is highly dependent on the values of the Integrity Support Message (ISM) parameters, including nominal measurement biases b_{nom}, standard deviations of the ephemeris and clock errors $\sigma_{URA}/\sigma_{URE}$, P_{sat} and P_{const}. The ISM values in Table 4 are determined based on GPS performance, but they may be optimistic for other constellations. If the constellations are subject to larger ISM values, the ARAIM navigation performance will be degraded (Lee and Bian, 2017). However, as sensitivity analyses to the ISM are beyond the scope of this paper, the same ISM values will be applied for all constellations for simulation purposes.

5.1. *Achievable V-ARAIM performance using only FD.* The goal of this first analysis is to quantify achievable V-ARAIM navigation performance over various numbers of the constellations. This addresses the impact of increased measurement redundancy on navigation integrity. The analysis is carried out to answer the following questions: whether adding more measurements always helps improve navigation performance, and what service levels

https://doi.org/10.1017/S0373463318000383 Published online by Cambridge University Press

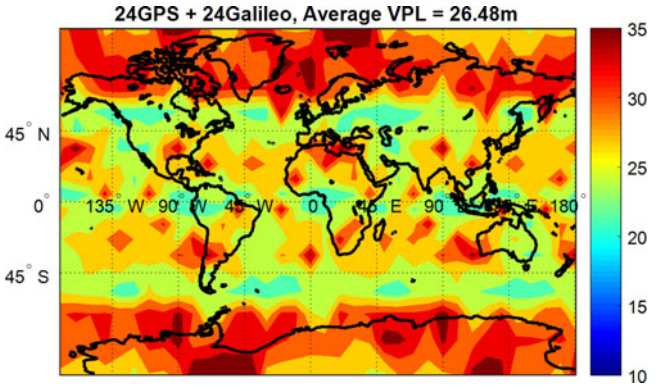


Figure 4. Achievable VPL levels (in metres) using two-constellation V-ARAIM detection.

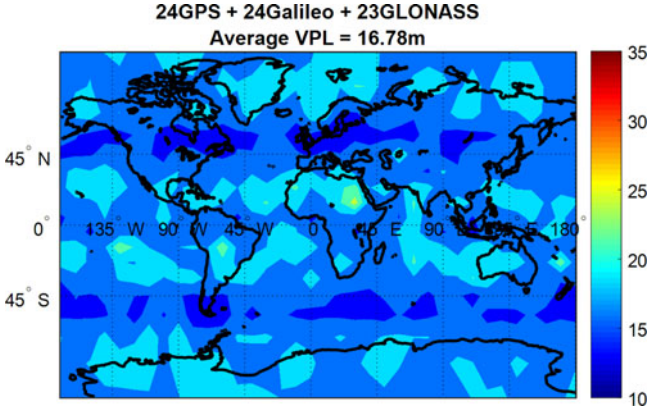


Figure 5. Achievable VPL levels (in metres) using three-constellation V-ARAIM detection.

Table 5. 99·5% availability coverage.

VAL	Two Constellations	Three Constellations	Four Constellations
15m	0%	14%	94·75%
20m	0%	97%	100%
35m	98·37%	100%	100%

can be achieved. Figures 4 to 6 demonstrate the achievable Vertical *PL* (*VPL*) with two, three and four constellations.

Table 5 expresses the performance in terms of availability coverages with varying VAL. Availability is defined as the fraction of time the navigation system is usable before the operation is initiated, and the coverage reflects the fraction of users in the investigated region that have availability greater than 0·995. Because VAL is the most stringent requirement criterion, it is used to determine V-ARAIM availability. The results indicate that adding constellations significantly improves V-ARAIM navigation integrity. With four constellations, high coverage can be achieved for VAL as low as 15 m.

https://doi.org/10.1017/S0373463318000383 Published online by Cambridge University Press

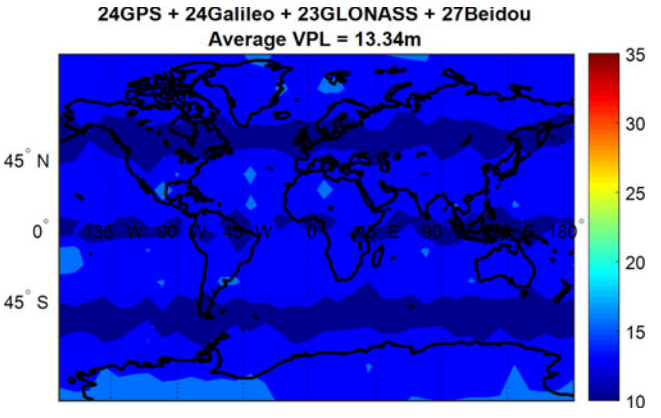


Figure 6. Achievable VPL levels (in metres) using four-constellation V-ARAIM detection.

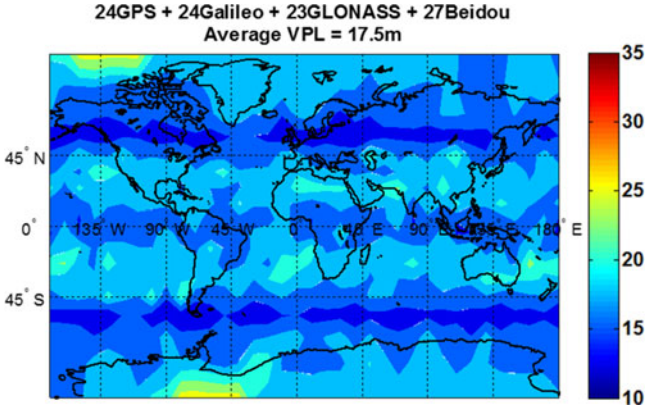


Figure 7. VPL map (in metres) using four-constellation V-ARAIM FDE.

5.2. *Overall ARAIM performance using both detection and exclusion.* The second analysis validates the exclusion scheme and shows the ARAIM availability while meeting both the integrity and continuity requirements. In Section 3 (Figures 1 and 2), we identified specific scenarios that required V-ARAIM exclusion to improve continuity using four constellations. Figure 7 shows that 100% availability coverage for LPV-200 can be achieved for V-ARAIM FDE, when the continuity requirements, in addition to integrity, can be simultaneously met.

Figure 8 illustrates worldwide availability performance for RNP 0·1 using dual-constellation H-ARAIM FDE. The result indicates that even with two constellations, our proposed exclusion scheme (including the exclusion function itself and corresponding integrity risk bound) can provide high availability while fulfilling H-ARAIM integrity and continuity requirements.

https://doi.org/10.1017/S0373463318000383 Published online by Cambridge University Press

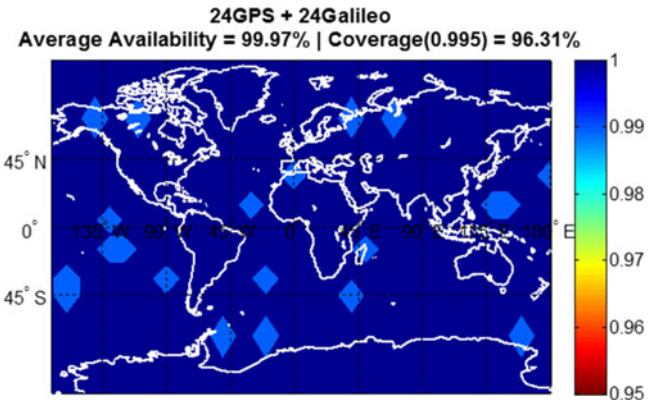


Figure 8. Availability map using dual-constellation H-ARAIM FDE.

6. CONCLUSION. This paper comprehensively investigates the fault exclusion problem in future multi-constellation, dual-frequency ARAIM. The key contribution is the establishment of a theoretical basis to quantify the contributions of fault events on continuity risk, thereby allowing quantitative assessment of the exclusion function performance relative to specific continuity requirements. We first interpret the continuity requirements for two important ARAIM-intended operations and investigate the impact of GNSS faults in the context of these requirements. It is concluded that an airborne H-ARAIM exclusion function is always required to improve continuity, whereas V-ARAIM exclusion is likely to be needed only if four constellations are applied and/or the constellations are subject to large fault probabilities. Accordingly, a real-time exclusion algorithm has been designed, its implementation process clarified and the associated FDE integrity risk bound derived. The results of the analyses show that, for V-ARAIM, adding more GNSS measurements could significantly improve navigation integrity. In addition, implementing the proposed exclusion scheme provides high availability for both V- and H-ARAIM, while simultaneously meeting integrity and continuity requirements.

ACKNOWLEDGMENTS

The authors would like to thank the Federal Aviation Administration for sponsoring this work. The authors would also like to thank Dr. Juan Blanch and Dr. Todd Walter from Stanford University for their advice. The views and opinions expressed in this paper are those of the authors and do not necessarily reflect those of any other organisation or person.

FINANCIAL SUPPORT

This work was supported by the Federal Aviation Administration (grant number DTFAWA-16-X-00004).

REFERENCES

Blanch, J., Walter, T. and Enge, P. (2010). RAIM with Optimal Integrity and Continuity Allocations under Multiple Failures. *IEEE Transactions on Aerospace and Electronic Systems*, **46**, 1235–1247.

https://doi.org/10.1017/S0373463318000383 Published online by Cambridge University Press

Blanch, J., Walter, T. and Enge, P. (2014). Exclusion for Advanced RAIM: Requirements and a Baseline Algorithm. *Proceedings of the 2014 International Technical Meeting of The Institute of Navigation*, San Diego, California, 99–107.

Blanch, J., Walter, T., Enge, Per., Lee, Y., Pervan, B., Rippl, M., Spletter, A. and Kropp, V. (2015). Baseline Advanced RAIM User Algorithm and Possible Improvements. *IEEE Transactions on Aerospace and Electronic Systems*, **51**, 713–732.

Blanch, J., Walter, T. and Enge, P. (2016). A Simple Satellite Exclusion Algorithm for Advanced RAIM. *Proceedings of the 2016 International Technical Meeting of The Institute of Navigation*, Monterey, California, 239–244.

Cassel, R. (2017). *Real-Time ARAIM Using GPS, GLONASS, and Galileo.* M.S. Thesis, Dept. of Mechanical, Materials, and Aerospace Engineering, Illinois Institute of Technology, Chicago, IL.

EU-U.S. Cooperation on Satellite Navigation, Working Group C. (2016). *ARAIM Technical Subgroup Milestone 3 Report*. http://www.gps.gov/policy/cooperation/europe/2016/working-group-c/ARAIM-milestone-3-report.pdf

FAA. (2010). *Phase II of the GNSS Evolutionary Architecture Study*, FAA report, Feb. 2010. https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/library/documents/media/GEASPhaseII_Final.pdf

FAA. (2012). *System Specification for the Wide Area Augmentation System*. FAA-E-2892d.

Gibbons, G. (2012). Munich Summit Charts Progress of GPS, GLONASS, Galileo, Beidou GNSSes. *Inside GNSS*, March 20, 2012. http://www.insidegnss.com/node/2981

Heng, L., Gao, G. X., Walter, T. and Enge, P. (2012). Automated Verification of Potential GPS Signal-In-Space Anomalies Using Ground Observation Data. *Proceedings of IEEE/ION PLANS 2012*, Myrtle Beach, South Carolina, 1111–1118.

ICAO. (2009). Annex 10, Aeronautical Telecommunications, Volume 1 (Radio Navigation Aids), Amendment 84.

Joerger, M., Stevanovic, S., Chan, F-C., Langel, S. and Pervan, B. (2013). Integrity Risk and Continuity Risk for Fault Detection and Exclusion Using Solution Separation ARAIM. *Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation*, Nashville, TN, 2702–2722.

Joerger, M., Chan, F.-C. and Pervan, B. (2014). Solution Separation Versus Residual-Based RAIM. *NAVIGATION*, **61**(4), 273–291.

Joerger, M. and Pervan, B. (2016). Fault Detection and Exclusion Using Solution Separation and Chi-Squared RAIM. *IEEE Transactions on Aerospace and Electronic Systems*, **52**, 726–742.

Lee, Y. C. (1986). Analysis of Range and Position Comparison Methods as a Means to Provide GPS Integrity in the User Receiver. *Proceedings of the 42nd Annual Meeting of The Institute of Navigation*, Seattle, WA, 1–4.

Lee, Y. and McLaughlin, M. (2007). Feasibility Analysis of RAIM to Provide LPV-200 Approaches with Future GPS. *Proceedings of the 20th International Technical Meeting of the Satellite Division of The Institute of Navigation*, Fort Worth, TX, 2898–2910.

Lee, Y. and Bian, B. (2017). Advanced RAIM Performance Sensitivity to Deviation of ISM Parameter Values. *Proceedings of the 30th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2017)*, Portland, OR, 2338–2358.

Milner, C., Bang, E., Macabiau, C. and Estival, P. (2017). Methods of Integrity Risk Computation for ARAIM FDE. *Proceedings of the 30th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2017)*, Portland, OR, 2371–2387.

Parkinson, B.W. and Axelrad, P. (1988). Autonomous GPS Integrity Monitoring Using the Pseudorange Residual. *NAVIGATION*, **35**(2), 255–274.

Pervan, B., (1996). *Navigation integrity for aircraft precision landing using the Global Positioning System*. Ph.D. Dissertation, Dept. of Aeronautics and Astronautics, Stanford Univ., Stanford, CA.

RTCA Special Committee 159, (1991). *Minimum Operational Performance Standards for Airborne Supplemental Navigation Equipment Using Global Positioning System (GPS)*. *RTCA/DO-208*.

US DOD. (2008). *Global Positioning System Standard Positioning Service Performance Standard*. Assistant Secretary of Defense for Command, Control, Communications and Intelligence. http://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf

Walter, T., Blanch, J., Joerger, M. and Pervan, B. (2016). Determination of Fault Probabilities for ARAIM. *Proceedings of IEEE/ION PLANS 2016*, Savannah, GA, 451–461.

Zhai, Y., Joerger, M. and Pervan, B. (2015). Continuity and Availability in Dual-Frequency Multi-Constellation ARAIM. *Proceedings of the 28th International Technical Meeting of The Satellite Division of the Institute of Navigation*, Tampa, Florida, 664–674.

https://doi.org/10.1017/S0373463318000383 Published online by Cambridge University Press

Zhai, Y., Joerger, M. and Pervan, B. (2016). H-ARAIM Exclusion: Requirements and Performance. *Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation*, Portland, Oregon, 1713–1725.

Zhai, Y., Joerger, M. and Pervan, B. (2017). Bounding Continuity Risk in H-ARAIM FDE. *Proceedings of the ION 2017 Pacific PNT Meeting*, Honolulu, Hawaii, 20–35.

APPENDIX - DERIVATION OF EQUATIONS TO COMPUTE FDE THRESHOLDS.

As described in Section 4.1, a detection event occurs (D_0) when any of the first layer detection statistics exceeds the thresholds, that is: $\bigcup_{d=1}^{n} |q_d| > T_d$. An LOC event occurs when the fault cannot be excluded ($\bar{E}_0$) - that is, when no exclusion option can be validated. In mathematical terms, this happens when a second layer detection occurs: $\bigcap_{e=1}^{n} \left(\bigcup_{k=1}^{n_e} |q_{e,k}| > T_{e,k} \right)$.

For H-ARAIM, Equation (9) in the main context can be written as:

$$P_{FANE,H} < P\left(\bigcup_{d=1}^{n} |q_d| > T_d | H_0 \right) P_{H_0} \tag{A1}$$

$$< \sum_{d=1}^{n} P(|q_d| > T_d | H_0) P_{H_0} \leq P_{FF,H,REQ} \tag{A2}$$

Therefore, the detection thresholds T_d for H-ARAIM can be computed using an inverse tail probability function of the standard normal distribution $Q^{-1}\{\cdot\}$:

$$T_d = Q^{-1}\left\{ \frac{P_{FF,H,REQ}}{2P_{H_0} \cdot n} \right\} \tag{A3}$$

which is the same as Equation (13).

Similarly, the exclusion thresholds $T_{i,j}$ are evaluated based on $P_{FP,H,REQ}$. Equation (10) becomes:

$$P_{FDNE,H} < \sum_{i=1}^{n} P\left(\bigcap_{e=1}^{n} \left(\bigcup_{k=1}^{n_e} |q_{e,k}| > T_{e,k} \right) | H_i \right) P_{H_i} + P_{NM} \tag{A4}$$

$$< \sum_{i=1}^{n} P\left(\bigcup_{k=1}^{n_e} |q_{i,k}| > T_{i,k} | H_0 \right) P_{H_i} + P_{NM} \tag{A5}$$

$$< \sum_{i=1}^{n} \sum_{k=1}^{n_e} P\left(|q_{i,k}| > T_{i,k} | H_0 \right) P_{H_i} + P_{NM} \leq P_{FP,H,REQ} \tag{A6}$$

where P_{NM} denotes the summation of prior probabilities for all non-monitored fault modes. The bound used in the transition from Equation (A4) to Equation (A5) is noteworthy, where only one exclusion option, associated with the correct fault hypothesis is considered, that is, $e = i$. Since the actual fault is excluded, the second layer detection statistics in Equation (A6) are fault free (H_0). Equation (A6) can be applied to set the exclusion thresholds over all the monitored fault hypotheses. In this work, we use an even allocation of $P_{FP,H,REQ}$ over all the hypotheses. Therefore,

$$T_{i,k} = Q^{-1}\left\{ \frac{P_{FP,H,REQ,Hi}}{2 \cdot n_e} \right\}, \quad \text{where } P_{FP,H,REQ,Hi} = \frac{P_{FP,H,REQ}}{n \cdot P_{H_i}} \tag{A7}$$

which is the same as Equation (14).

https://doi.org/10.1017/S0373463318000383 Published online by Cambridge University Press