Advanced RAIM Architecture Design and User Algorithm Performance in a real GPS, GLONASS and Galileo scenario

Ilaria Martini, Markus Rippl and Michael Meurer
German Aerospace Center DLR, Germany

BIOGRAPHIES

Ilaria Martini received the Master Degree in telecommunication engineering and the Ph.D. in information technology from the University of Florence, Italy. She was at the Galileo Project Office of ESA/ESTEC in 2003, working on the performance of the Galileo Integrity Processing Facility. She was research associate in 2004 at the University of Florence and in 2005 at the Institute of Geodesy and Navigation of the Federal Armed Forces Germany in Munich. In 2006 she joined the navigation project department of Ifen GmbH in Munich. Since 2012 she works as research associate in the Institute of Communication and Navigation at the German Aerospace Center (DLR), Oberpfaffenhofen. Her main area of interest is GNSS Integrity Monitoring.

Markus Rippl received his Diploma in Electrical Engineering and Information Technology from Technische Universität München (TUM) in 2007. Since then, he has been a research associate with the Institute of Communications and Navigation (IKN) at the German Aerospace Center (DLR), in Oberpfaffenhofen near Munich. His field of work is the integrity of GNSS-based navigation using receiver-side algorithms.

Michael Meurer received the diploma in electrical engineering and the Ph.D. degree from the University of Kaiserslautern, Germany. After graduation, he joined the Research Group for Radio Communications at the Technical University of Kaiserslautern, Germany, as a senior key researcher, where he was involved in various international and national projects in the field of communications and navigation both as project coordinator and as technical contributor. From 2003 till 2005, Dr. Meurer was active as a senior lecturer. Since 2005 he has been an Associate Professor (PD) at the same university. Additionally, since 2006 Dr. Meurer is with the German Aerospace Center (DLR), Institute of Communications and Navigation, where he is the director of the Department of Navigation and of the center of excellence for satellite navigation.

ABSTRACT

In the past years the scientific community is investigating with increasing interest innovative techniques to provide vertical guidance to aviation users up to precision approach and even autonomous guidance on ground. Next to SBAS and GBAS systems other novel architectures have been under investigated. In particular the ARAIM concept is based on the fact that the future of multiconstellation and multifrequency signals will offer the possibility to reduce the dependency from the ground infrastructure and consequently reduce further the deployment and operation costs. The user will be provided with an augmentation signal (Integrity Support Message) updated and transmitted with a long latency. This is the idea of the Advanced Receiver Autonomous Monitoring.

This paper proposes an architecture which aims on one hand to maximize the reuse of existing infrastructure and on the other to provide the user with the necessary robustness required mostly in the early next years by new constellations. The differentiating factor among the different alternatives is the so called Time to ISM Alarm, the update frequency and dissemination of the ISM information. The proposed architecture foresees the provision of two different type of messages: a long term one addressing nominal conditions and a short term one to detect anomaly conditions.

The paper presents also the user algorithms suitable for this architecture which optimizes the user availability by reducing the protection level with respect to existing solutions. The performance of the user algorithm has been analysed in a real scenario: a receiver in front of an airport hangar disturbed by a GNSS repeater. The paper shows how the user algorithm can detect the disturbance and reject it. Furthermore the protection level performances is also shown, and in particular its improvement with respect to existing ARAIM algorithm [1].

I. INTRODUCTION

The design of the Integrity Support Message (ISM) Architecture enabling the fulfilment of the aviation precision approach requirements for a standalone GNSS receiver with Advanced Receiver Autonomous Integrity Monitoring techniques is an interesting and challenging topic. This paper aims to contribute to the discussion proposing an ARAIM architecture design and an user algorithm suitable for the proposed architecture.

This introduction describes the context and the ARAIM design factors addressed by the approach proposed in the second section. Secondly the architecture and the user algorithm are detailed in the second section. Finally a measurement campaign where the proposed algorithms were validated with real GPS, GLONASS and Galileo constellation is described in the third section.

1) Integrity Requirements for aviation users: The objective of the ARAIM concept is to provide the aviation users with vertical guidance up to precision approach based on multi-constellation GNSS signals. Navigation systems supporting vertical guidance of aircraft are subject to several requirements governing their performance. The requirements are standardized through the International Civil Aviation Organization (ICAO). The target operation levels are LPV, LPV-200 and beyond, which are specified in the ICAO Standards And Recommended Practices SARPs [2], as follows (Selection of the criteria):

- Fault-free vertical accuracy 4m at 95% and 10m at 10^{-7},
- Faulty-case vertical accuracy 15m at 10^{-5},
- Vertical error bound 15m at the $0.5\cdot$ integrity risk[1] (Vertical Alert Limit VAL),
- Integrity risk $2 \cdot 10^{-7}$ per approach (150s),
- Time-to-Alert (TTA) 6 seconds.

These represent some of the most strict requirements for GNSS applications at the present. They refer to small percentiles (10^{-7}) and to short operation intervals (approach duration of 150s), on which the user must be alerted within 6s when a failure condition occurs.

2) Advanced RAIM Architecture and Design Drivers: The ARAIM concept was proposed within the U.S. GPS Evolutionary Architecture Study report [3]. Further evolution has been provided by the Working Group C ARAIM Technical Subgroup Interim Report [4]. The proposed receiver algorithm is based on the Multiple Hypothesis Solution Separation method described by [1].

The new concept of ISM/ARAIM represents an interesting possibility to meet the strict LPV integrity requirements. At present the architecture design is an open topic, containing several alternatives still to be screened.

Many aspects influence and determine the optimum design: liability constrains of the Aviation Navigation Service Providers (ANSP) and GNSS Providers, politic agreement among states and certification-standardization authorities, economic aspects related to the need to reuse as much as possible existing infrastructure, etc. This paper will focus only on the technical aspects.

The main ISM Architecture design drivers are the followings:

- the monitoring network in charge of collecting the observables used to compute the ISM content. Its coverage might be global (e.g. GNSS sensor stations network or IGS network with suitable service and commitment level), regional (e.g. SBAS like network) or local (e.g. GBAS like monitoring stations),
- the dissemination network in charge of sending the ISM to the final user. Its coverage might also be global (e.g. GNSS constellation), regional (GNSS constellation transmitting regional information, or subset of a GNSS constellation, e.g. orbiting only on a specific region, or GEO satellites) or local (VHF data link like VHF Data Broadcasting link of GBAS),
- the ISM latency, i.e. ”the time it takes for the ground network to identify an issue in the space segment and alert the aircraft to that issue” [1],
- the Constellation Service Provider commitment, that is the responsibility taken by the GNSS service provider in guaranteing a certain level of required performance,
- the ASNP regulatory requirements, that ability from each country and region to delegate risk of operations.

Not all the combinations of the previous alternatives are feasible. Most of them do not provide the desired performance. The following sections analyze and identify technical constrains and proposes a design optimization.

II. ADVANCED RAIM ARCHITECTURE

This section provides a description of the ARAIM architecture with a focus on the ground subsystem. The purpose of the ground system in ARAIM is to provide integrity parameters to the users, known as the Integrity Support Message (ISM). As opposed to classical RAIM [5] where these parameters are fixed assumptions on the signal-in-space (SIS) performance, the ARAIM architecture is more flexible: A dedicated ground system monitors GNSS performance and adapts the integrity parameters. Depending on the particular architecture, these updates can either be executed at a higher rate in the range of hour or minutes, at longer intervals, or only when needed (conserving the long latency nature). Generally, the update intervals will always be longer than the TTA requirement of 6 seconds. The rate of updates determines the level of performance that can be obtained (more frequent updates allow for less overestimation of the errors and thus less conservatism in the integrity threat models), but small latency of these updates also increases the operational cost of the infrastructure (Required data links during flight of aircraft).

In contrast to the majority of other proposals (e.g. [1]), this paper uses a combination of long-term and short-term monitoring to maximize the obtainable system performance. The two kinds of Integrity Support Messages (ISM) that are sent to the user are:

- An ISM with a long latency in the order of months, or only updated when needed. This message could be disseminated using terrestrial (VDB) or satellite based (GEOs, or GNSS) means,
- A second ISM with a shorter latency in the order of minutes to hours. Depending on the interval, different dissemination strategies become available: Delivery of the ISM at dispatch for intervals longer than the flight duration, or data link based updates either from terrestrial

---

[1] Precisely the integrity risk defines the probability that either the vertical error or the horizontal error is above the limit without notification. A possible partition of the risk is the allocation of $0.5P_{HMI}$ to vertical, other partitions use more risk for vertical and less for horizontal. The proposed algorithm in fact does not perform such a partition at all.

(VDB) or satellite based (GEOs, or GNSS) data transmitters when the aircraft is in the arrival/approach phase at the destination airport.

The low-latency ISM is used to monitor baseline assumptions on the Signal-In-Space Error (SISE) such as the distribution of its nominal magnitude and the likelihood that a fault occurs, invalidating the nominal error model. The short-latency ISM adds a short-term upper bound on the actual SISE.

The user algorithm can either apply only the information provided by the long-term monitoring part of the architecture, or both the long-term and the short-term messages. This flexibility is obtained by allocating a partition of the threats either to the short-term monitoring or to the user algorithm, depending on ISM availability. This allocation is reflected in a different test threshold of the FDE algorithm. This threshold depends on the update rate of the short term ISM. Once a possible range of values for the update rate has been defined, the corresponding FDE threshold can be described as a lookup table and hardcoded in the receiver. The ARAIM performance is better when current ISM short-term data is available, in fact the user detection requirements are relaxed and the availability improves. And the increased level of complexity at receiver level is acceptable.

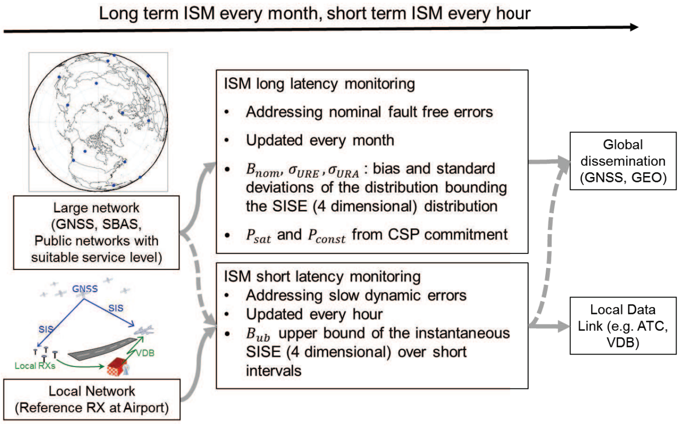

Fig. 1. ARAIM Architecture design

A. Long latency ISM

The long latency ISM aims to provide the user with information on the system behaviour in nominal conditions. Using this information the user can estimate the risk due to nominal errors. The monitoring network providing the long term ISM is a global sparse network able to process multiconstellation multifrequency signals. Suitable ground networks would be the ground segments of the GNSS, or SBAS or networks like IGS if the data is available at an adequate service level and with the required committment. The distribution of the ground network receivers must be sufficient to observe all satellites at all times at a geometric diversity that allows for separation of 3-D ephemeris biases and clock biases.

The update rate for the long-term ISM data is in the order of one month or can be updated only when necessary. In particular the information provided to the user are[2]:

- B_{nom}: bias of the distribution bounding the nominal SISE
- σ_{URA}: standard deviation of the distribution bounding the SISE
- P_{sat}: satellite failure probability, i.e. probability that the nominal error model is invalid
- P_{const}: constellation failure probability

The information on the SISE distribution, that is B_{nom} and σ_{URA} are provided in the satellite domain, specifying the long-track, cross-track, radial and clock components. If the link bandwidth does allow it, the covariance matrix for these values should be provided, that means including the extradiagonal cross-correlation components. In case of bandwidth constrains then the scalar values should be foreseen. As the dissemination may be sporadic, no continuous link is necessary. Possible candidates for transmission of the long-term ISM are:

- GNSS in-band dissemination
- GEOs, in particular including the data into SBAS messages
- Local area data links at dispatch of the aircraft and/or at gate of originating airport
- The NAV database found within aircraft Flight Management Systems (FMS), which is today updated at a 28 days interval.

It is highlighted that the long term monitoring does not provide the error bounding through re-estimation of the satellite orbit and clock but by monitoring the validity of the URA and SISA navigation message values and inflate them if they do not perform a proper error bounding.

The probability of SISE exceeding the threshold T can be denoted as

$$\begin{aligned}
&P(|SISE| > T) = \\
&P(|SISE| > T|\sigma_T \leq \sigma_{URA})P(\sigma_T \leq URA)+ \\
&P(|SISE| > T|\sigma_T \leq \sigma_{URA}) \\
&P(\sigma_T \leq \sigma_{URA})P(\sigma_T > URA)+ \\
&P(|SISE| > T|\sigma_T > \sigma_{URA}) \\
&P(\sigma_T > \sigma_{URA})P(\sigma_T > URA).
\end{aligned} \tag{1}$$

where σ_T indicates the true standard deviation of the SISE, σ_{URA} the long latency ISM information and the URA the bounding value of the navigation message.

The first term

$$P(|SISE| > T|\sigma_T \leq \sigma_{URA})P(\sigma_T \leq URA) \tag{2}$$

represents the case in which the navigation message information URA performs a correct bounding. This case is covered by the user algorithm in the protection level estimation.

The second one

$$P(|SISE| > T|\sigma_T \leq \sigma_{URA})P(\sigma_T \leq \sigma_{URA})P(\sigma_T > URA) \tag{3}$$

---

[2] Note that all the estimates obtained from ground monitoring are established per satellite. The index i referring to a particular satellite is omitted here and in the subsequent sections for simplicity.

represents the case in which URA is not properly bounding but the ISM information σ_{URA} does allowing a correct protection level estimation by the user.

Finally the third one

$$P(|SISE| > T|\sigma_T > \sigma_{URA})P(\sigma_T > \sigma_{URA})P(\sigma_T > URA) \tag{4}$$

is the remaining risk, when both the GNSS and ARAIM ground monitoring fail in providing a correct bounding of the satellite orbit and clock errors. There is no possibility to control this term with additional monitoring. So the only possibility is to keep this term small with respect to the 10^{-7} integrity requirement. As it can be noted, the product of the two must be $< 10^{-7}$ and not each of them. But this significant advantage is only ensured if the ARAIM ground monitoring performs a bounding monitoring. Instead if it performs a navigation message re-estimation then the σ_{URA} must satisfy alone the integrity requirements. This might be a critical aspect for a new deployed architecture, in particular dealing with new constellations, because a long data history is needed to reach the required confidence level.

The objective of the long-term ground monitoring can thus be split into two parts, which are subsequently detailed: The estimation of the nominal error model and the verification of satellite fault rates and constellation fault rates.

1) Estimation of nominal Signal-in-Space Error (SISE) parameters: The MHSS ARAIM user algorithm provides integrity by estimation of an upper bound for the position error. The fundamental assumption for a robust bound is a conservative model of the range error distribution, i.e. the likelihood that the error magnitude of a specific range measurement is larger than a specific number. MHSS assumes maximum biases and Gaussian error distribution overbounds for the range measurements, and the task of the ground monitoring subsystem is to obtain the model parameters from data. These parameters are the Gaussian overbound σ_{URA} (User Ranging Accuracy) and a maximum nominal bias B_{nom}.

The Gaussian overbound σ_{URA} needs to be valid for very small tail probabilities in the order of 10^{-7} or less. Consequently, a large number of uncorrelated samples is necessary to obtain the required confidence. The bias is not connected with an explicit excess probability. Consequently, under nominal conditions, $|SISE - B_{nom}|$ is overbounded by a Gaussian distribution with standard deviation σ_{URA}.

2) Verification of satellite & constellation fault rates: The second objective of the ground network is to verify the fault rates of satellites and constellations. These fault rates denote the likelihood that the nominal SISE model as described above is not valid. The probability is defined for the duration of an approach, 150s, and refers to a single satellite. The ARAIM concept is based on a certain level of commitment from the CSP, in particular in the satellite failure probability characterization. The value P_{sat} and P_{const} could be provided by the CSP in the format of Service Performance Commitment. The ARAIM ground monitoring has then only the role to assess their correctness and robustness. This operation can be performed only on long batch of data and updated on a monthly basis.

An explicit and additional risk of constellation fault is defined by P_{const}. This probability refers to the case that a large set of satellites, or the complete constellation, are simultaneously affected by a common fault. Examples for these faults are mismodeling of ephemeris parameters such as the earth orientation w.r.t. the inertial frame (Earth Orientation Parameter), or failures cause by improper operation of the ground segment.

3) Connection of nominal SISE parameters and fault rates: The connection between these two sets of parameters is, for a single satellite

The probability that the distribution of SISE is not bounded by a Gaussian distribution with mean value B_{nom} and standard deviation σ_{URA} is contained in the satellite failure probability P_{sat}.

B. Short latency ISM

The short latency ISM on the other side can additionally protect the ARAIM user in case an anomalous condition occurs. In particular it aims to monitor and detect errors which don't change with respect to the short term update rate. It is then designed to protect against slow dynamic errors. The only content of the short-term ISM is for each satellite an upper bound of the SISE on the short term ISM validity interval, B_{ub}.

The underlying concept of this approach is the division of the single satellite fault threat space into two parts: One that evolves slow enough so that users may be alerted before the error effect becomes hazardous, and an another partition covering faults with a higher dynamic, effectively only to be mitigated by genuinely receiver autonomous methods. This division is obtained by modeling possible faults according to their physical origin and assigning probabilities individually. This separation process is closely connected to the maximum possible latency of the short-term channel.

All faults that can not be observed by the ground monitoring have to be considered at the user level. These faults are handled at receiver algorithm level, in particular an FDE detection scheme is applied as a barrier to those threats.

The update rate can be in order of order of one hour, or possibly longer if the separation of slow-dynamic and fast-dynamic threats allows for detecting a significant part of the errors in more long-term scenarios.

1) Relation of slow-dynamic error detection and satellite fault rate: The satellite fault rate, P_{sat}, is an estimate of the likelihood that the nominal SISE error model is not valid for a specific satellite. In conventional MHSS algorithms this probability is used to determine the likelihood of a fault hypothesis, i.e. a unique combination of assumed faults within the set of available range measurements. Every likely fault hypothesis is considered as one possible solution, and thus a position estimate is computed excluding the potentially faulted satellites. The impact of these potential faults on the position estimate is attributed by including all partial solutions into a protection level interval.

With the proposed extension of the user algorithm the user can already determine the worst-case impact of a non-nominal SISE on the position solution, if it can be observed by the short-term ground monitoring. The corresponding probability of those specific faults consequently need not be considered in the MHSS hypothesis. The P_{sat} determined by long-term monitoring thus has to cover only fast-dynamic non-nominal SISE threats.

Previously, a flexible operation mode of the user algorithm was proposed where either only long-term monitoring or with both ISM types available. To provide robust modeling of the threat space, the long-term monitoring thus would theoretically need to estimate two sets of P_{sat} parameters for every satellite: A likelihood that any non-nominal fault occurs for users that use only the long-term monitoring, and a likelihood that fast dynamic errors occur for those users that use the slow-dynamic threat observation function of the short-latency component.

In fact in case of only long term ISM the satellite failure probability is as follows

$$P_{sat} = \sum_{i=1}^{N_T} P_{T_i} \tag{5}$$

where N_T indicates the whole number of threats and P_{T_i} the state probability of the *i-th* threat. If also the short term ISM is used, then the satellite failure probability becomes

$$P_{sat} = \sum_{j=1}^{N_{HDT}} P_{T_j} + \sum_{k=1}^{N_{SDT}} P_{T_k} P_{MD,k}^{ARAIM} \tag{6}$$

where N_{HDT} and N_{SDT} respectively are the number of high-dynamic and slow dynamic threats.

With a short term monitoring, the slow dynamic threats would be included with a reduced state probability (original one multiplied by the ARAIM ground monitoring missed detection probability, P_{MD}^{ARAIM}). It is observed that this distinction of the satellite failure probability a negligible impact at user level for the protection level equations. In fact this value is used to estimate the failure mode probability, which weight the corresponding subset protection level. A small variation of the P_{sat} has a negligible impact and would require the transmission to the user of the P_{MD}^{ARAIM}) values. For this reason the use algorithm proposed considers conservatively the long latency satellite failure probability 5.

The impact has instead to be considered at FDE algorithm level, where a reduced risk can be allocated to this monitoring with an increased missed detection probability.

2) Estimation of the upper bound of instantaneous SISE: The upper bound B_{ub} refers to the worst case SISE that might be effective for any user within the service volume, at any time instant during the validity period of the short-term ISM. It is comprehensible that only faults with known time-characteristics can be monitored that way. These fault types can include:

- Clock runoffs with an observable clock drift rate
- Ephemeris errors that result in ephemeris errors slowly building up

All these faults might be classified as either unobservable or observable, depending on their rate - only if the SISE ramp builds up slow enough it can be guaranteed that users can be successfully alerted.

Furthermore the upper bound, B_{ub}, takes into account also the ARAIM ground monitoring estimation accuracy as shown in figure 2. This is necessary to avoid having to transmit also this information to the user, which would be otherwise needed in the protection level equation.

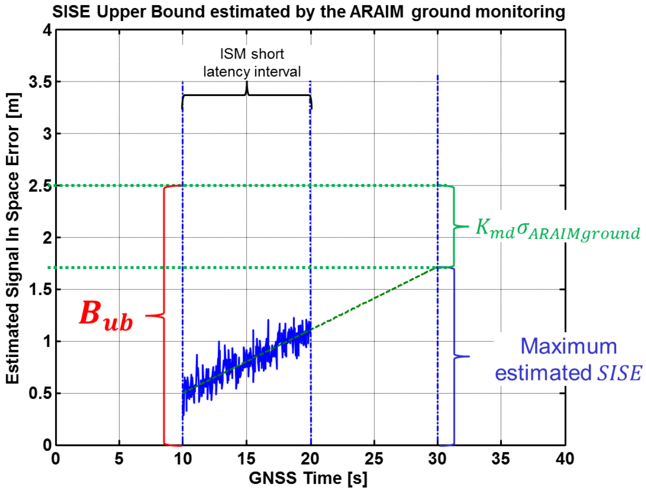

Fig. 2. ARAIM ground monitoring process to estimate the error upper bound.

3) Motivation for dual monitoring approach: The introduction of the short term ISM introduces of course an additional element and then a further degree of complexity, but is motivated by the following advantages:

- New constellations will have an initial long phase where ISM operators may desire to limit the confidence assigned to the GNSS operators' performance figures. In this phase it is necessary to support the user as much as possible in detecting any failure condition. Since the ARAIM architecture should be as independent as possible from a ground monitoring, the best trade off for the ISM latency between its detection capability and its requirements on the architecture should be used.
- A short term ISM is a further degree of freedom for each ASNP. Independently short term monitors could be provided depending on the authority region and the provider. The user algorithm remains compatible with worldwide environments, using different integrity risk allocation depending on the scenario. This would be reflected in different threshold values for the FDE, which can be hardcoded as a lookup table in the receiver. This solution also enables simplicity of the receiver design, implementing only one algorithm.
- Having a monitor with a shorter update rate allows the relaxation of the user requirements. In fact the user

FDE algorithm will be tuned according to a predefined probability of missed detection. This probability depends on the overall integrity risk allocation and in particular takes into account that the product of the prior fault probability and the missed detection probability must be smaller that the allocated part of the integrity risk. Now introducing an additional monitoring at ARAIM ground segment level part of the threats will be detected and monitored on ground, as shown in 4. The effect is a reduced threat occurrence probability. The final result is an improvements in terms of availability.

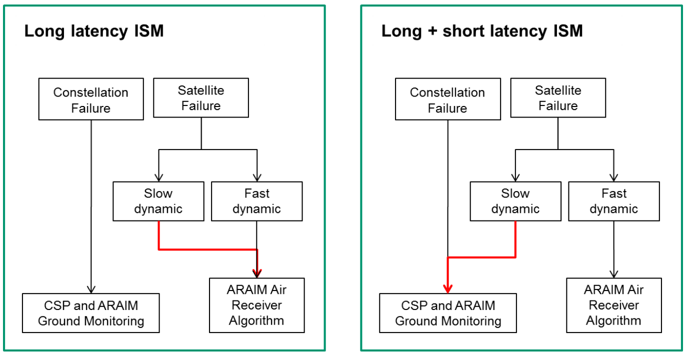

Fig. 3. Threat allocation among GNSS, ARAIM ground monitoring and user

The architecture characteristics and properties are summarized in Table I.

TABLE I

ARAIM Architecture Characteristics

ISM type	Content	Latency	Monitoring Network	Dissemination
Long term	bias and standard deviation of long term constellation nominal errors	1 month	global (ISM, GNSS, SBAS)	global (GNSS, SBAS)
Short term	upper bound of the short term constellation failures	1 hour	global (ISM, GNSS, SBAS) or local	global (GNSS) or local (VDB)

III. USER ALGORITHM

The algorithm proposed and described in this paper has many similarities with [1], but presents the following important differences:

- The solution separation approach MHSS is used only for the Fault Detection and Exclusion (together with the χ^2 test [1]) but not for the estimation of the protection level, where instead the short term ISM information is used to model the errors. With this approach the advantage is that in the failure condition cases, where the MHSS approach excludes the failing satellites to estimate the subset solution, this algorithm uses all the satellites: for the failing satellite it uses a degraded model (with a mean value B_{ub} from the short term ISM instead of B_{nom} from the long term ISM). The advantage is that the overall protection levels are reduced and the availability improves, as shown in the next section,
- The integrity of the user is estimated not computing the protection level to be compared with the Alert Limit, but computing the integrity risk, that is directly the tail area delimited by the Alert Limit. The advantage is that there is no need in this approach to allocate statically the integrity risk between the vertical and horizontal components.

The user ARAIM algorithm is constituted by the following steps:

- Covariance matrix estimation
- Position estimation
- Computation of the maximum number of simultaneous faults affecting the integrity risk
- Fault detection and exclusion
- Computation of the fault-free and faulty biases and covariance matrixes
- Integrity risk estimation and comparison with the requirement threshold

These steps are detailed in the following[3]:

A. Covariance matrix estimation

The covariance matrix C is defined as follows ([1])

$$C(i,i) = \sigma^2_{URA,i} + \sigma^2_{tropo,i} + \sigma^2_{user,i} \tag{7}$$

where $\sigma_{URA,i}$ is the standard deviation of the satellite orbit and clock errors and is contained in the Integrity Support Message. $\sigma_{tropo,i}$ is the standard deviation of the tropospheric delay modelled which is expressed according to [6] as

$$\sigma_{tropo}(\theta) = 0.12\left(\frac{1.001}{\sqrt{0.002001 + (\sin(\frac{\pi\theta}{180}))^2}}\right) \tag{8}$$

with θ the elevation angle expressed in degrees. The standard deviation of the receiver noise, σ^{GPS}_{user}, is modelled according to [7]

$$\sigma^{GPS}_{user} = \sqrt{\frac{f^4_{L1} + f^4_{L5}}{(f^2_{L1} - f^2_{L5})^2}}\sqrt{\sigma^2_{MP} + \sigma^2_{Noise}} \tag{9}$$

$$\sigma_{MP}(\theta) = 0.13 + 0.53e^{-\frac{\theta}{10}} \tag{10}$$

$$\sigma_{Noise}(\theta) = 0.15 + 0.43e^{-\frac{\theta}{6.9}} \tag{11}$$

---

[3] In the following steps the B_{nom} and σ_{URA} indicates scalar values in the range domain. But if actually they are designed in the satellite domain (long-track, cross-track, radial and clock component), as previously suggested, a projection on the specific user range domain must be performed as preliminary step.

B. Position estimation

The position solution is obtained by means of a least square linear estimation as described in [8]. In particular, for the linear observation equation

$$\underline{\rho} = \underline{H}\underline{x} + \underline{\varepsilon} \tag{12}$$

where $\underline{x}$ is the vector containing the user position offset in ECEF and user clock offset, the $\underline{\rho}$ contains the pseudorange measurements, the solution is

$$\underline{x} = \underline{S}\underline{\rho} \tag{13}$$

$$\underline{S} = (\underline{H}^T \underline{C}^{-1} \underline{H})^{-1} \underline{H}^T \underline{C}^{-1} \tag{14}$$

The position covariance matrix is

$$\underline{\Sigma} = (\underline{H}^T \underline{C}^{-1} \underline{H})^{-1} \tag{15}$$

and the same matrix in a local reference system (east, north and up) is obtained with a rotation matrix $\underline{R} = \{\underline{e}_{east}, \underline{e}_{north}, \underline{e}_{up}\}$, that is

$$\underline{S_{enu}} = \underline{R}^T \{(\underline{H}^T \underline{C}^{-1} \underline{H})^{-1} \underline{H}^T \underline{C}^{-1}\}_{submatrix(3,N)} \tag{16}$$

$$\underline{\Sigma}_{enu} = (\underline{S}_{enu} \underline{C} \underline{S}^T_{enu}) \tag{17}$$

$$\underline{\Sigma}_{enu} = \begin{pmatrix} \sigma_e & \sigma_{en} & \sigma_{eu} \\ \sigma_{en} & \sigma_n & \sigma_{nu} \\ \sigma_{eu} & \sigma_{nu} & \sigma_u \end{pmatrix} \tag{18}$$

C. Computation of the maximum number of simultaneous faults affecting integrity risk

This algorithm computes the probability that a certain number of satellites have simultaneously a failure and check whether this is negligible with respect to the overall integrity risk requirement. This algorithm computes also the probability of having a certain number of simultaneous failures, i.e the probability of each combination with narrow fault P_{NF}, as well as the probability of a faulty free system P_{FF}. The reference algorithm is described in detail in [1].

D. Fault detection and exclusion

This algorithm detect anomalous range error using two tests: a solution separation test and chi square test. A suitable algorithm for this part is also described in detail in [1].

E. Computation of the fault-free and faulty biases and covariance matrixes

After the positioning and the fault detection and exclusion the receiver has to estimate the integrity parameters. For this purpose it uses a model based on the information provided by the ISM.

In fact there are several possibilities depending on the number and the combination of simultaneous satellite failures. Each failure combination is considered separately and the relative integrity risk estimated. The final integrity risk is then the sum of all the contribution.

The model for the fault free satellites is assumed to follow a Gaussian distribution in the range domain with nominal bias as provided by the long term ISM

$$\epsilon_{range,FaultFree,i} \sim \tag{19}$$

$$N(B_{nom,i}, \sqrt{\sigma^2_{URA,i} + \sigma^2_{tropo,i} + \sigma^2_{user,i}}) \tag{20}$$

The error model in the position domain after projection in the east, north and up reference system, is

$$\epsilon_{enu,FaultFree} \sim N(\mu_{enu,FF}, \underline{\Sigma}_{enu,FF}) \tag{21}$$

where

$$\mu_{east,FF}(i) = |S_{topo}[1,i]|\, B_{nom}(i) \tag{22}$$

$$\mu_{north,FF}(i) = |S_{topo}[2,i]|\, B_{nom}(i) \tag{23}$$

$$\mu_{up,FF}(i) = |S_{topo}[3,i]|\, B_{nom}(i) \tag{24}$$

The model for the faulty satellites is also assumed to follow a Gaussian distribution in the range domain with the upper bound as contained in the short term ISM

$$\epsilon_{range,Faulty,i} \sim N(B_{ub,i}, \sqrt{\sigma^2_{tropo,i} + \sigma^2_{user,i}}) \tag{25}$$

Since the upper bound contains already the ARAIM ground monitoring estimation accuracy and also an estimation of the maximum satellite orbit and clock errors, the range error standard deviation is constituted only by the tropospheric and the receiver noise.

All failure combinations are considered up to the maximum number of simultaneous failure as previously estimated. For this narrow failure case all the signals are characterized as fault free except for the failing satellites for which the fault mode is considered.

In the position domain after projection in the east, north and up reference system, the position error model is

$$\epsilon_{enu,Faulty,j} \sim N(\mu_{enu,NF}, \underline{\Sigma}_{enu,NF}) \tag{26}$$

where

$$\mu_{east,NF}(i) = |S_{topo}[1,i]|\, B_{ub}(i) \tag{27}$$

$$\mu_{north,NF}(i) = |S_{topo}[2,i]|\, B_{ub}(i) \tag{28}$$

$$\mu_{up,NF}(i) = |S_{topo}[3,i]|\, B_{ub}(i) \tag{29}$$

$$\mu_{hor,NF}(i) = \sqrt{\mu^2_{east,NF}(i) + \mu^2_{north,NF}(i)} \tag{30}$$

The standard deviation in the horizontal position plane is the following

$$\alpha_{hor} = \sqrt{\frac{\sigma_e^2 + \sigma_n^2}{2} + \sqrt{\left(\frac{\sigma_e^2 - \sigma_n^2}{2}\right)^2 + \sigma_{en}^2}} \tag{31}$$

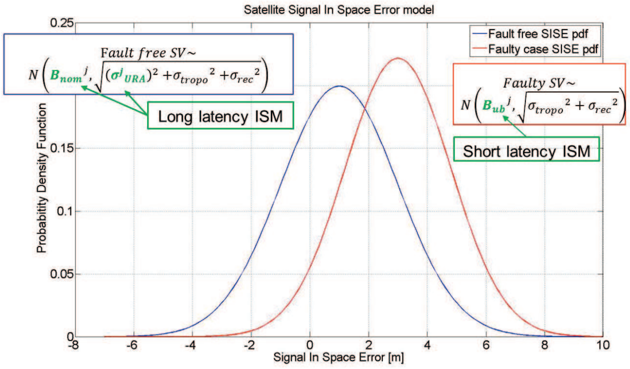

Fig. 4. SISE model based on long and short latency ISM

F. Integrity risk estimation and comparison with the requirement threshold

The assurance of the vertical error bound, that is the integrity risk probability, is finally constituted by the following contributions

$$P_{HMI,vert}(VAL) = P_{HMI,vert,FF}(VAL) + \tag{32}$$

$$\sum_{i=1}^{N_{FailureMode}} P_{HMI,vert,NF,i} \tag{33}$$

$$\begin{aligned} P_{HMI,vert}(VAL) = & \left\{ Q\left(\frac{VAL - \mu_{FF}}{\sigma_{u,FF}}\right) + \right. \\ & \left. Q\left(\frac{VAL + \mu_{FF}}{\sigma_{u,FF}}\right) \right\} P_{FF} + \\ & \sum_{i=1}^{N_{subset}} \left\{ Q\left(\frac{VAL - \mu_{NF}}{\sigma_{u,NF}}\right) + \right. \\ & \left. Q\left(\frac{VAL + \mu_{NF}}{\sigma_{u,NF}}\right) \right\} P_{NF}(i) \end{aligned} \tag{34}$$

The horizontal error bound is guaranteed by

$$\begin{aligned} P_{HMI,horz}(HAL) = & \left\{ Q\left(\frac{HAL - \mu_{FF}}{\alpha_{u,FF}}\right) + \right. \\ & \left. Q\left(\frac{HAL + \mu_{FF}}{\alpha_{u,FF}}\right) \right\} P_{FF} + \\ & \sum_{i=1}^{N_{subset}} \left\{ Q\left(\frac{HAL - \mu_{NF}}{\alpha_{u,NF}}\right) + \right. \\ & \left. Q\left(\frac{HAL + \mu_{NF}}{\alpha_{u,NF}}\right) \right\} P_{NF}(i) \end{aligned} \tag{35}$$

with the cumulative distribution function of a non-central χ^2-distribution with degree of freedom 2 (argument x and non-centrality parameter λ):

$$cdf_{\chi^2}(x, \lambda) = \int_0^x pdf_{\chi^2}(t, \lambda) dt \tag{36}$$

$$pdf_{\chi^2}(x, \lambda) = \frac{1}{2} e^{-\frac{1}{2}(x+\lambda)} \sum_{i=0}^{\infty} \frac{x^i \lambda^i}{2^{2i}(i!)^2} \tag{37}$$

The overall integrity risk is finally compared with the requirement threshold in order to assess the service availability: the service is in fact not available in case the integrity risk is not ensured to be smaller than the requirement threshold of $P_{HMI,vert} + P_{HMI,hor} \leq 10^{-7}$.

IV. ALGORITHM VALIDATION WITH A MULTICONSTELLATION MULTIFREQUENCY SCENARIO

The algorithm has been validated with real data collected with a multiconstellation multifrequency receiver. In particular the receiver could track GPS, GLONASS and also three Galileo satellites[4]. All the measurements were collected and processed on two frequencies (L1 and L5).

In order to validate with real data an integrity algorithm, it would be necessary to insert satellite orbit and clock feared events in the received signals. Since there is no possibility to artificially manipulate the navigation signals, a work around was found for this research. A GNSS repeater was used to deteriorate the signals. In fact the DLR has a flight experimentation center with aircraft used for research purpose. Inside the hangar hosting the DLR aircraft there is a GNSS repeater used for indoor positioning and instrument testing.

GNSS repeaters largely disturb GNSS receivers which are in the proximity of the hangar and represent a source of interference to be detected and eliminated. Authorities have recently been investigating in detail the topic, particularly after a series of service interruptions caused by a GNSS repeater have been observed at the Hannover airport in Germany [9].

The measurement campaign was performed in two phases of one hour each. During the first one the GNSS repeater was switched off and the receiver was outside the hangar with the door opened in a static configuration. During this phase the receiver was calibrated observing its performance in nominal condition. In the second phase the GNSS repeater was switched on and the receiver started moving. The receiver was moved approaching the hangar and then in the opposite direction. This procedure had the scope to create situations where a subsets of measurements were tracking the satellites through the direct path and part of them through the repeater.

The goal was in fact to create an inconsistency among the measurements, which can be detected by the ARAIM FDE algorithm. A further goal was to estimate the protection level and in particular to compare the performance of the ARAIM algorithm based on a long term ISM described in [1] with the one proposed in this paper based on the use of a short term ISM.

A. Scenario description

Figure 5 shows the field where the measurement campaign was performed. The hangar has a GNSS repeater inside, whose sending antenna is located on the roof inside the hangar as

---

[4] During the measurement campaign all 4 Galileo IOV satellites were actually visible but one of them was not transmitting any signal

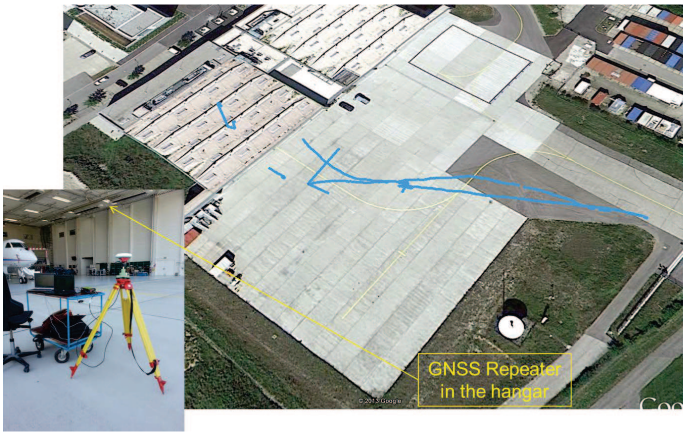

Fig. 5. Measurement campaign at the DLR airport hangar where a GNSS repeater was disturbing the multiconstellation receiver

shown in Figure 5. The GNSS repeater retransmits the signals with a 55dB amplification. The receiver was a JAVAD Sigma GNSS receiver based on a TRIUMPH Chip, configured to track GPS, GLONASS and Galileo dual frequency L1 and L5 signals.

The measurements were processed with dual frequency iono-free linear combination, troposphere model and positioning according to the MOPS processing chain [8]. The reference data were generated with a commercial software performing a PPP with precise IGS orbit, clocks and ionex data.

Figure 6 shows the sky plot in the first phase when the repeater was switched off and the hangar door was closed. The hangar was blocking the reception of all the signals coming from north-west. Whereas with the repeater switched on and the hangar door opened also satellites behind the hangar become visible (Figure 7).

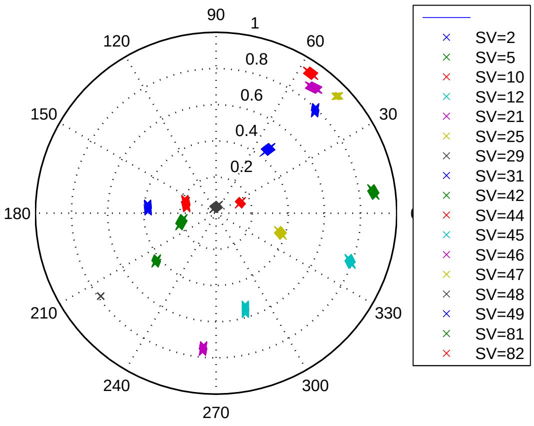

Fig. 6. Sky plot with the repeater switched off and the hangar door closed. According to the Universal Satellite Indexes standard, $PRN <= 37$ for GPS, $38 <= PRN <= 70$ for GLONASS and $PRN >= 71$ for Galileo

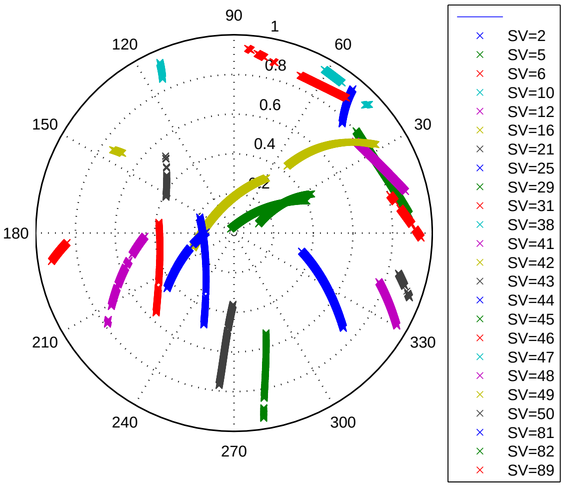

Fig. 7. Sky plot with the repeater switched on and the hangar door opened. According to the Universal Satellite Indexes standard, $PRN <= 37$ for GPS, $38 <= PRN <= 70$ for GLONASS and $PRN >= 71$ for Galileo

B. ARAIM configuration and settings

The Advanced RAIM was configured with the following ISM values:

- $B_{nom} = 0.5m$
- $\sigma_{URA} = 0.75[m]$ for GPS and Galileo and $\sigma_{URA} = 1[m]$ for GLONASS
- $\sigma_{URE} = 0.5 \cdot \sigma_{URA}$
- $B_{ub} = maxSISE + K_{md}\sigma_{ground} = 10 + 5.19 \times 0.99[m]$
- $P_{sat} = P_{const} = 10^{-4}$

C. Failure detection

The effect of the GNSS repeater on the receiver can be appreciated in Figure 8.

When the repeater is switched on the receiver starts tracking the signals coming from the repeater instead those from the direct path. When all the signals are tracked from the repeater, as it happens in the indoor positioning case, the PVT algorithm provides the position of the repeater receiving antenna. Beside the estimated clock offset contains the delay due to the distance between the receiver and the repeater (and the eventual re-transmission delay). Usually not all tracking loops change from tracking the SV signal to tracking the repeated signal at the same time. In particular in our scenario satellites with high elevation and their line of sight close to the hangar (e.g PRN 5) happened to start being tracked through the repeater before other signals. The effect in the specific case is displayed in Figure 8: satellite (PRN 5) presented a significantly larger range error with respect to the others (in the order of 100m). After few seconds the receiver started tracking all the signals from the repeater. The effect can be appreciated in the common jump in all the range errors.

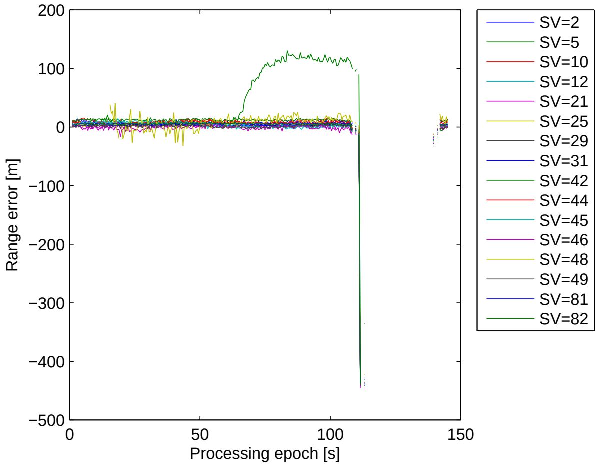

Fig. 8. Range error, computed as the difference between the measured range, corrected for the propagation error and the clock offsets, and the true range

Figure 9 shows the effect on the PVT solution in particular for the user clock offset estimation. The clock offset absorbs the biases due to the distance between the receiver and the repeater, as shown in Figure 9.

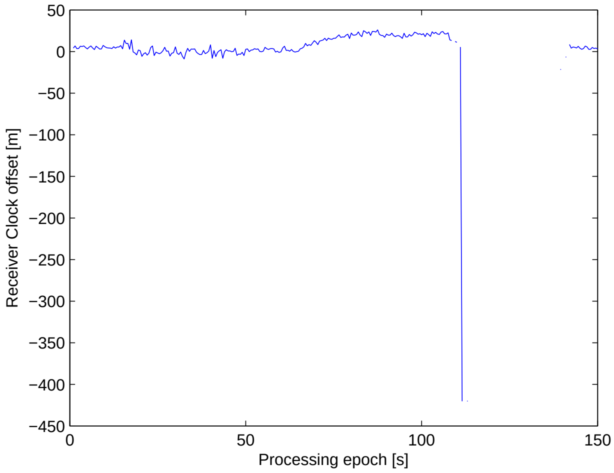

Fig. 9. User clock offset estimation error

It is highlighted that the clock offset estimation is degraded in the interval of time in which the the PRN 5 has a large range error.

Also the residuals shows the anomaly, as displayed in Figure 10.

The ARAIM algorithm in particular the FDE part is able to detect the anomalous condition of PRN 5 and set an invalid satellite flag, as shown in Figure 11 (value 1 indicates excluded satellites).

The FDE algorithm can detect correctly the failure condition and improve the positioning performance. In particular the clock offset error is not anymore affected by the PRN 5

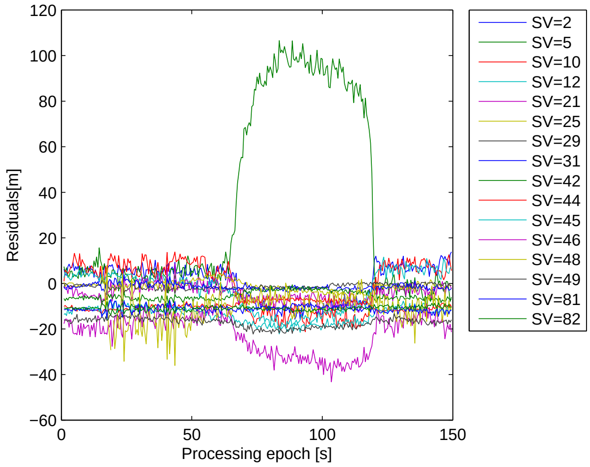

Fig. 10. PVT residuals, defined as the difference between measured pseudorange, processed for propagation errors and satellite clock errors and the estimated range

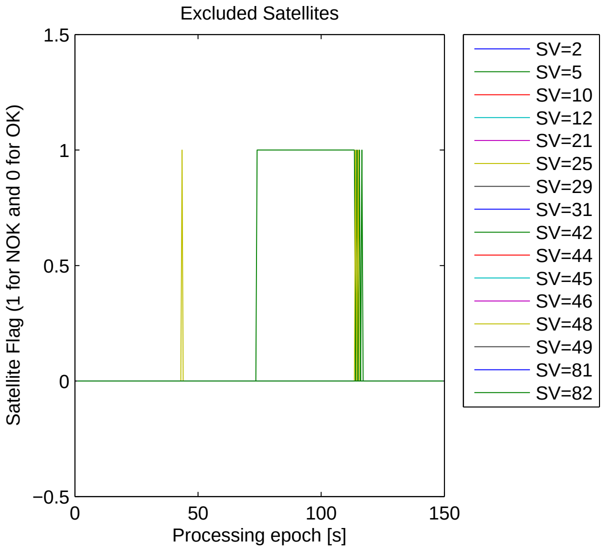

Fig. 11. Satellite flag output of the FDE algorithm: 1 for satellite excluded and 0 for fault free satellites

anomaly, as it can be appreciated comparing Figure 9 with Figure 12.

The position error is significantly improved as it is shown by comparing Figure 13 with Figure 14 and Figure 15 with Figure 16.

The results demonstrated and confirmed the capability of the ARAIM FDE algorithm to protect the users against errors in the ranging signals.

D. Protection Level comparison

The second part of the measurement campaign aimed to assess and compare the performance of the ARAIM integrity estimation of the following two alternatives:

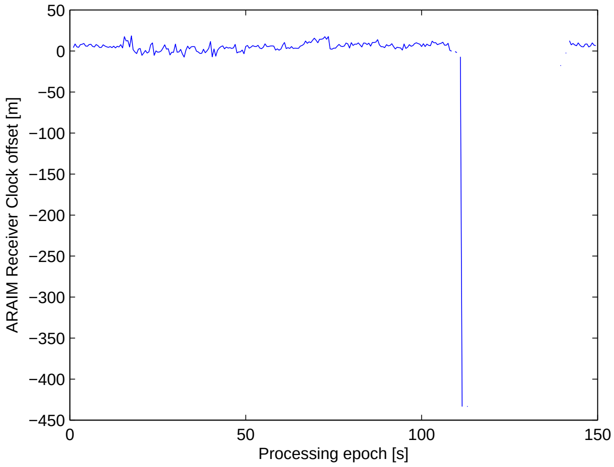

Fig. 12. User clock offset estimation error after satellite exclusion performed by the FDE algorithm

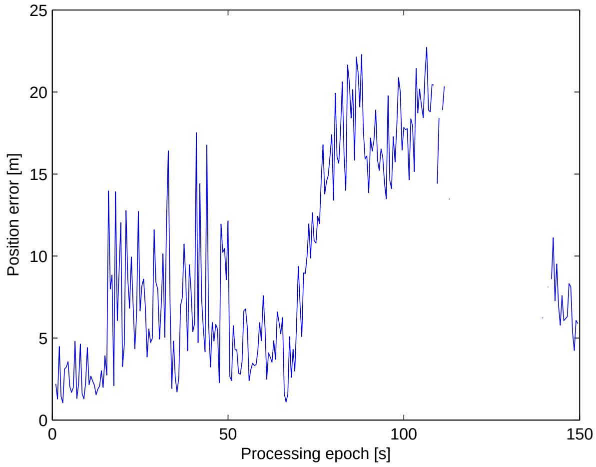

Fig. 13. Difference between the PVT estimated position and the true reference position.

- the ARAIM algorithm, presented in [1], based on a long term ISM and on a MHSS approach
- the ARAIM algorithm, presented in this paper, based on the combination of a long term with a short term ISM. The short term part is used to model the faulty satellites without using a subset reduced geometry as foreseen by the MHSS approach.

The protection levels time series and histograms are displayed respectively in Figure 17 and Figure 18[5].

The improvement in terms of reduced protection level was confirmed by the real data results. The reduction of the protection level is ensured by the fact that for each failing condition the whole geometry is used, instead of a reduced one of a constellation subsets. The fault in the satellite is modelled considering an increased bias (B_{ub}), which anyway does not have a large effect on the protection level in comparison to the geometry degradation of the MHSS approach. In fact although the short term ISM used as input value was significantly large (in the order of 10m), the algorithm proposed provided smaller protection levels. This measurement campaign showed that including the short term monitoring allows modelling properly the errors to ensure the necessary integrity service and at the same time allows avoiding the degradation of service availability caused by the conservatism of the MHSS approach.

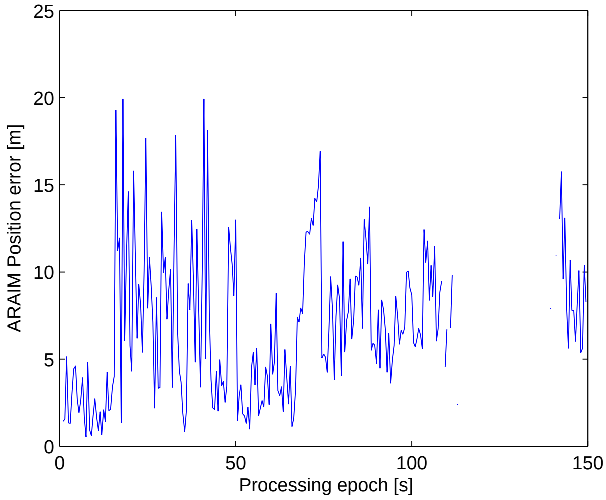

Fig. 14. Difference between the ARAIM estimated position and the true reference position.

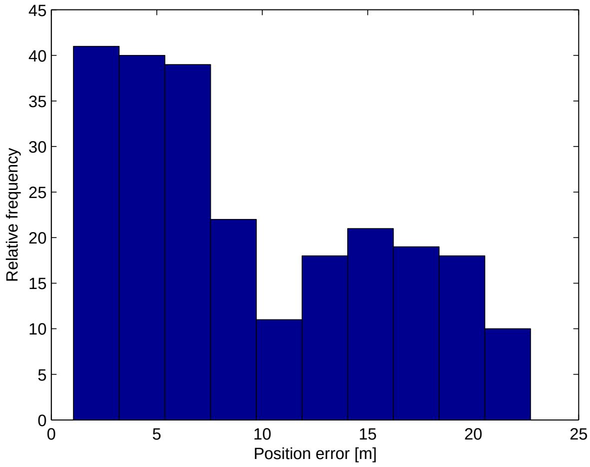

Fig. 15. Histogram of the difference between the PVT estimated position and the true reference position.

V. CONCLUSION

The Advanced RAIM architecture aims to provide aviation users with vertical guidance up to precision approach with

---

[5] As described in the previous section the algorithm presented in this paper estimates the integrity risk instead of the protection level. In order to compare the performances of the two alternatives, for the second alternative the equivalent value of the protection level was derived from the integrity risk estimation (with a Q-inverse function)

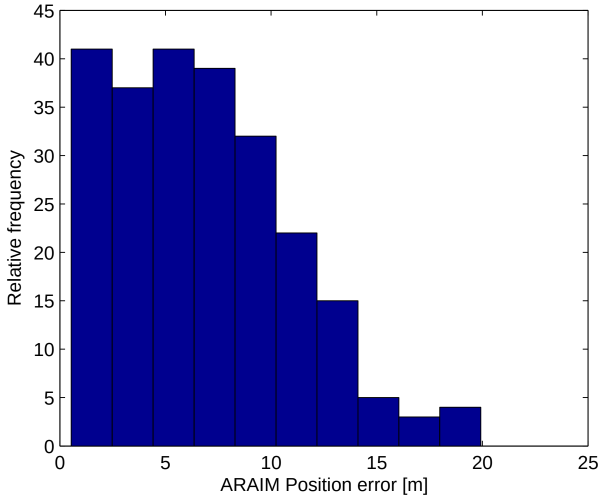

Fig. 16. Histogram of the difference between the ARAIM estimated position and the true reference position.

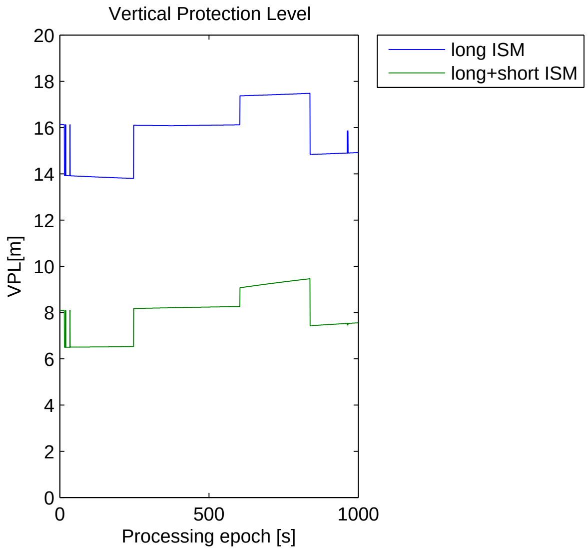

Fig. 17. Protection level time series: performance comparison between the ARAIM algorithm presented in this paper and the one described in [1].

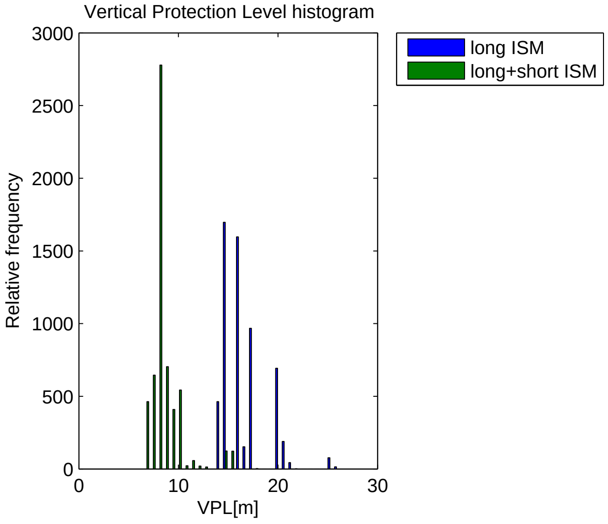

Fig. 18. Protection level histograms: performance comparison between the ARAIM algorithm presented in this paper and the one described in [1].

the minimal dependency from the ground monitoring. This challenging task has to face the difficulties related to new constellations: reticence to meet a service commitment from the Constellation Service Provider due to the lack of history data and the confidence on the system. On the other side it has also to provide worldwide compatibility while a regional or local sovereignty from each ASNPs. All these difficulties, if not correctly handled, risk to delay significantly the introduction of this technology.

This paper proposes an alternative ARAIM Architecture which is based on the combination of a long term and a short term augmentation information (ISM). Besides it presents the user algorithm suitable for this architecture. The advantages of this design with respect to others are interesting. It allows each ASNP to reuse existing trusted and certified infrastructure (local monitoring or dissemination network). Each ASNP can use a different update rate for the short term ISM allowing an important system flexibility. It relaxes the user requirements in detecting failure conditions improving the position availability (of primary importance for new constellation where many unexpected unknown threats will arise in the first years of operation). It provides a simplified user algorithm, which remains worldwide compatible even if the short term ISM present several update rate.

The proposed user algorithm was validated with a three constellation scenario (GPS, GLONASS, Galileo) and using a GNSS repeater of the DLR flight experiment center to generate system anomalies. The presented algorithm demonstrated its robustness in detecting the failure conditions and improving the position accuracy. Furthermore the proposed algorithm provided a significant improvement in terms of protection level, improving service availability with respect to existing user algorithms.

References

[1] J. Blanch, T. Walter, P. Enge, Y. Lee, B. Pervan, M. Rippl, and A. Spletter, “Advanced RAIM User Algorithm Description: Integrity Support Message Processing, Fault Detection, Exclusion, and Protection Level Calculation,” in *Proceedings of the ION GNSS 2012*, 2012.

[2] International Civil Aviation Organization (ICAO), “Annex 10, Aeronautical Telecommunications, Volume I (Radio Navigation Aids),” 2005.

[3] FAA GEAS Panel, “Phase II of the GNSS Evolutionary Architecture Study,” Feb. 2010.

[4] Bilateral EU-US ARAIM Technical Sub Group of the Working Group C, “GPS-Galileo Working Group C ARAIM Technical Subgroup Interim Report (Issue 1.0, 19 December 2012),” tech. rep., 2012.

[5] T. Walter and P. Enge, “Weighted RAIM for Precision Approach,” in *Proceedings of the ION GNSS Conference 1995*, ION, 1995.

[6] “Airborne Supplemental Navigation Equipment Using the Global Positioning System (GPS), Technical Standard Order (TSO), C-129,” Dec 1992.

[7] "RTCA/DO-208: Minimum Operational Performance Standards for Airborne Supplemental Navigation Equipment Using Global Positioning System (GPS)," 1991.

[8] "RTCA/DO-229D: WAAS Minimum Operational Performance Specification (MOPS)," 1991.

[9] E. Steindl, W. Dunkel, A. Hornbostel, C. Haettich, and P. Remi, "The impact of interference caused by GPS repeaters on GNSS receivers and services," in *Proceedings of the European Navigation Conference (ENC), Vienna*, 2013.