# Ephemeris Failure Rate Analysis and its Impact on Category I LAAS Integrity

L. Gratton, R. Pramanik, H. Tang, B. Pervan, *Illinois Institute of Technology*

**ABSTRACT**

One of the integrity concerns for the Local Area Augmentation System (LAAS) is the ephemeris threat scenario. The responsibility of detecting such failures lies on the LAAS Ground Facility (LGF). It is essential for the system to provide monitor functions that minimize the integrity risk, while not affecting the availability and continuity levels significantly. At the very first stage of the monitor analysis, it is necessary to use an ephemeris Failure Rate (*FR*) in order to derive the monitor requirements. This paper derives a *FR* from rigorous analysis of the GPS performance standards to ensure that the rate used is conservative. The *FR* is further supported using archived ephemeris data from the last 10 years. The detailed analysis necessary to obtain the *FR* also leads to a new requirement to ensure integrity: the need of a solid notification channel between GPS and the LGF for failures and maneuvers. In case that reliable notification link cannot be established, some threats would remain unmitigated. Ideas on monitors that could potentially solve this problem are presented on this paper, as well as initial results on simulations to establish their effectiveness.

**INTRODUCTION**

One of the integrity concerns for the Local Area Augmentation System (LAAS) is the ephemeris threat scenario. The responsibility of detecting such failures lies with the LAAS Ground Facility (LGF). It is essential for the LGF to provide monitor functions that minimize the integrity risk, while not affecting the availability and continuity levels significantly.

At the very first stage of the monitor analysis and design, it is necessary to use an ephemeris Failure Rate (*FR*) in order to derive the monitor requirements, the main one being the allowable Probability of Missed Detection ($P_{MD}$). The value used for *FR* in previous studies varies from $3.6 \times 10^{-3}$ to $10^{-4}$ per ephemeris change. This *FR* was shown to be sufficiently small for some monitors to function effectively (the ones related to wrong ephemeris uploads, or "Type B," explained in detail in the next section) [1]; but the confidence on the correctness of this rate was never properly established. Furthermore in the analysis of ephemeris threat mitigation it became obvious that, if possible, it would be desirable to justify by probability arguments that certain monitors were not needed (the monitors related to maneuvers, or previously stored data at the LGF; known as "Type A" threats, also explained in detail in the next section). Unfortunately initial studies determined that a *FR* of $10^{-4}$ was not small enough to arrive to that conclusion. It then became crucial to establish a conservative but realistic *FR* that would help determine which monitors are needed and which are not, and whether sufficient integrity is provided with the implementation of these monitors.

There is no doubt that the GPS Operational Control Segment (OCS) is an efficient and reliable organization. However the difficulty resides in translating this confidence into numbers that can be used in requirement derivation and analysis. In this work the *FR* is derived from studying official documents, complemented with other sources to update information. These documents do not provide a *FR* for ephemeris failures, so one was deduced from a chain of conservative assumptions. Even though great care was put in ensuring the assumptions were conservative, it was necessary to verify this *FR* with real data. To do this, 10 years of ephemerides were analyzed in search of failures.

The *FR* obtained from this work proved to be smaller than what was previously assumed, however, the detailed chain of thought necessary to produce it, uncovered other Potentially Hazardous Events (*PHE*) besides an ephemeris failure. These are mainly planned maneuvers that are unknown to the LGF. The threat of such a "Missed Notification" (*MN*) has to be taken into account and is introduced in the analysis. Possible ways of mitigating this threat are introduced at the end of the paper.

**EPHEMERIS THREATS AND MONITORS**

The Category I LAAS ephemeris threat model considers three basic cases (Note: no attention should be given to the logic of the labeling, as it is inherited from the historical evolution of these definitions):

Type B: There is an error of significant magnitude in the current broadcast ephemeris, but the ephemerides from the previous two days are fault free. To mitigate Type B threats the LGF has reliable information (from stored ephemerides from the previous two days) that it can use to get an independent predictive estimate of the current ephemeris and compare it to the actual broadcast parameters [1]

Type A1: There is an error of significant magnitude in the current broadcast ephemeris, and there *is also* a potential error in ephemerides from previous days. The actual 'failure' is the same as for the type B threat (corrupt current ephemeris) but it is different in that the capability of the type B monitor to detect it is compromised by faulted data that is used by the monitor. It is worth noting that if the LGF detects a failure, becomes aware of a maneuver, or recieves an 'UNHEALTHY' message from the spacecraft, it will trigger a two day wait before using that satellite again (to allow storage of the ephemerides needed in the Type B monitor)

A faulty prior-day ephemeris could have two origins: an ephemeris that was originally faulty and was stored by the LGF, or an ephemeris that was correct when broadcast and stored, but then became outdated because of a maneuver of which the LGF was unaware (for example, a maneuver on the other side of the earth when the SV was not visible at the LGF).

Although a Type A1 Monitor concept exists [1], the software implementation is complicated and it would also require the use of carrier phase measurements, antenna phase pattern calibration, and LGF reference receiver baselines longer than 200 m [2]. For these practical reasons it is essential to perform a rigorous integrity analysis to determine whether an A1 monitor function is actually required or if the monitor can be simplified or omitted entirely. In an attempt to do that, we will analyze the *FR* and its impact on the monitor requirements.

Type A2: A fault free ephemeris is validated by the Type B monitor, and after this happens, a maneuver the LGF is unaware of occurs, rendering the ephemeris in use not representative of the SV orbit and making it a potential hazard for navigation.

The Type A2 threat could have two sources: the first one is a planned maneuver within sight of the LGF, during which the SV health bit is not turned to 'UNHEALTHY', and the LGF is unaware of the maneuver. (Note: an incident with these characteristics took place on April 10th 2007. [3]). The second possible source of an A2 threat would be a spontaneous firing of the thrusters of a satellite.

## IMPACT OF FAILURE RATE ON EPHEMERIS MONITORS

The Type B monitor is in a very advanced state of development, and the impact of the *FR* on its requirements and performance is very straightforward. If a *FR* of, for example $3.6\times10^{-3}$ was used to develop the monitor, if the derived *FR* is smaller than that value, all the analysis done for the development would be conservative, and this work's task regarding the monitor is finished.

The ephemeris type A1 threat monitor function is different from other monitors as it would not directly ensure integrity of data used in navigation. Instead, it would be used to validate ephemeris data on (prior) days 1 and 2 that will be used on (current) day 3 by another integrity monitor (Type B). For a Hazardously Misleading Event (*HMI*) to occur, a chain of events has to happen:

a. A Potentially Hazardous Event (*PHE*) has to occur on day one or two. A *PHE* could be a failure in the broadcasted (and stored) ephemerides from GPS, or a maneuver that renders the stored ephemeris useless.
b. No Detection of the *PHE* from the Operational Control Segment ($ND_{OCS}$), or a Missed Notification (*MN*) by the LGF
c. A failure on the current ephemeris on day 3 ($f_3$)
d. No Protection from the type B monitor for such failure (*NPB*)

The probability of events a-d occurring, and the relation between those probabilities will determine the Probability of *HMI* ($P_{HMI}$). In order to provide integrity to the system, $P_{HMI}$ has to be smaller than the integrity risk requirement for an A1 threat. Assuming an allocation for this risk of $2.07\times 10^{-8}$, we can translate these concepts into a formula:

$$P_{A1\backslash HMI} = P[NPB_3 \cap f_3 \cap (ND_{OCS} \cup MN) \cap (PHE_1 \cup PHE_2)] \le 2.07\times10^{-8} \quad (1)$$

To facilitate analysis, we can separate this joint probability into the product of conditional probabilities as follows:

$$P_{A1\backslash HMI} = P[A]\times P[B]\times P[C]\times P[D] \quad (2)$$

With:

$$A = PHE_1 \cup PHE_2$$
$$B = [ND_{OCS} \cup MN | (PHE_1 \cup PHE_2)]$$
$$C = [f_3 | (ND_{OCS} \cup MN) \cap (PHE_1 \cup PHE_2)]$$
$$D = [NPB_3 | f_3 \cap (ND_{OCS} \cup MN) \cap (PHE_1 \cup PHE_2)]$$

We can study each term in (2) separately.

Once the ability of the Type B monitor to detect failures is compromised by corrupt stored data, it is difficult to establish what the monitor can and cannot detect, so no credit is taken for integrity mitigation for the Type B monitor, which is equivalent to considering:

$$P[D]=1 \quad (3)$$

Determining the $P[C]$ depends on two things: the *FR* and its independence (or not) from event *B*. We will now concentrate on determining a conservative *FR*.

We must remember that the *FR* we are studying is an ephemeris failure rate exclusive of the GPS system; we are still not analyzing its impact on the LAAS user integrity. The obvious source for this value is the Global Positioning System Standard Positioning Service Performance Standards document (GPSSPSPS), which defines what can be expected from the system [4]. We cannot avoid getting into some details of the document to understand the strengths and weaknesses of our assumptions. Most useful information is in Appendix A (GPS Documented Performance Characteristics), which states "This Appendix is to be used for information only". In spite of this warning, we felt that this information was reliable and useful, as the document reads "…the Appendix defines …conservative expectations for GPS service reliability performance…".

.

The GPSSPSPS document recognizes only 3 types of failures: "GPS is designed to be fault tolerant. Most potential failures are either caught before they manifest themselves or are compensated by the system. The only failures to which the system seems susceptible are of 3 types: Insidious long term, catastrophic almost instantaneous and short term transients". The only ephemeris failures mentioned in the document are classified as "insidious long term.": Insidious-long term: "…do not propagate quickly, to date, have not affected support of SPS accuracy PS. Typically due to a problem in the ephemeris state estimation process."

The document states that 3 failures per year (for all three types of failures) is a conservative number, and that the expected number is 1 failure per year. The GPSSPSPS does not discuss abrupt ephemeris failures, but in light of the phrase "seems susceptible" (previous paragraph) we feel that they should be addressed. Since the failure rate for all three types of failures is less than 3/year, we conservatively assume that the GPS ephemeris *FR* is also 3/year. Then assuming the number of satellites in the constellation is 27, the number of ephemeris changes per day as 12, and taking into account that half of these failures will (probabilistically speaking) happen on the other side of the earth, where a particular LGF site will not see them, we establish our *FR* per ephemeris change per SV as:

$$FR = \frac{3f/yr}{365days/yr \times 12eph/day \times 27sv} \quad (4)$$
$$FR = 1.27 \times 10^{-5} f/eph/sv$$

We consider all the assumptions and interpretations of the GPSSPSPS document to be conservative, however, as our intent is to provide integrity, we will verify this result by observing real data in a separate section later in the paper.

The GPSPSPS states that errors above 30 m are detected with a maximum detection time of 6 hours; and the nominal detection time is 30-45 minutes. The maximum of 6 hours would be a problem for our Type B monitor. As a faulted ephemeris is broadcast for only 2 hours, it could be stored by the LGF (to be used on day 3), and the anomaly be detected by the OCS afterwards, without the LGF ever being notified. However some research determined that the 6 hour maximum was an outdated value reflecting the gaps on SV observation from the ground. It was confirmed from different sources that all SVs have a minimum of 2 monitoring stations observing them at all times [5],[6] and [7], so these gaps in coverage no longer exist.

Several important conclusions can be derived from the previous paragraph. The first one is related to the matter of independence we need to define $P[C]$. We can assume a *PHE* on days 1 or 2 will be detected by the OCS within 2 hours. (if it's a planned maneuver it is "detected" by definition); then, two possibilities are to be considered:
- The GPS OCS determines the cause of the failure, and in this case, it is logical to assume the likelihood of a failure on day 3 will be actually smaller than for days 1 or 2 as that particular failure cause will presumably be eliminated, or
- The cause of the failure is not determined: In that case we could assume the satellite will not be set healthy until the origin of the failure is established. From this reasoning, a failure on day 3 is deemed less likely to happen if there was a *PHE* on days 1 or 2. Then it is conservative to define:

$$P[C] = P[f_3 | (ND_{OCS} \cup MN) \cap (PHE_1 \cup PHE_2)] = P[f_3] = FR = 1.27 \times 10^{-5} \quad (5)$$

From the discussion above it can also be inferred that $P(ND_{OCS})$ is negligible. This follows from the fact that the OCS will detect any error bigger than 30 m and the errors that concern a LAAS user are of the order of 1000's of meters (as the user has the benefit of eliminating all errors in the line of sight with the LGF correction) [8]. Thus all failures that could produce an *HMI* are effectively detected by the OCS within 2 hours. We find no reason to believe the occurrence of a *PHE* would affect the channel of notification between GPS and the LGF, so we assume the two events are independent. We can now write:

$$P[B] = P[(ND_{OCS} \cup MN) \mid (PHE_1 \cup PHE_2)] = P[MN \mid (PHE_1 \cup PHE_2)] = P[MN] \quad (6)$$

We will assign a value to this term shortly.

$P[A]$ has two sources: A faulty ephemeris that was stored by the LGF (before the OCS detects the failure), or a maneuver executed after the ephemeris was stored, making the ephemeris no longer representative of the SV's orbit. $P[A]$ will consequently result from adding two terms, one for each of the sources of *PHE* mentioned above. Each of these terms will be composed by the Occurrence Rate (*OR*), times the Exposure Time (*ET*) corresponding to each case, times the number of SVs in view. For an ephemeris failure $OR_f = FR$, and for maneuvers we will assume $OR_M$ = 2maneuvers/SV/year [9]. For the *ET,* for the ephemeris failures we will use $ET_f$ = 2 days (or 24 ephemerides). [Note: It could be argued that only the ephemerides broadcast when the SV is in view should be considered, but we already used a multiplier of 0.5 when deriving the *FR*, and cannot take credit for the same thing twice]. For the maneuvers, we initially consider an exposure time of two days, as any maneuver would invalidate a stored ephemeris regardless of it being in view of the LGF or not. However, if any part of the maneuver is within sight of the LGF the LGF would observe the unhealthy message from that SV, thus triggering the two day wait of the Type B monitor. It is worth doing some preliminary analysis on this before writing the final formulas.

Consider a SV Pass Length *PL* (duration of time it is in sight of the LGF), and consider an SV Maneuver Duration *MD* (duration of time the SV is broadcasting an 'UNHEALTHY' message because of that maneuver). If any part of the *MD* coincides with *PL*, then the two day wait will be triggered, and all previously stored ephemerides will be discarded by the Type B monitor. Then, for each day, the Non Hazard Intervals (*NHI*) will be (see figure 1):

$$NHI = PL + 2 \times MD \quad (7)$$

This corresponds to the *PL* plus the duration of any hypothetical maneuver before or after the *PL* that has a common epoch with the *PL*.

The *PHE* Intervals (*PHEI*) for each day, will be the portion of the day that doesn't meet the common epoch condition stated above:

$$PHEI = 24hr - NHI \quad (8)$$

To obtain the values for the whole exposure time, we only need to multiply all terms by 2 (for 2 days). We are now interested in the times for which, if a maneuver happens during that time; the two day wait would not be triggered (as the LGF never observes the 'UNHEALTHY' message) thus causing a *PHE*. We can define it as the Percentage of time a maneuver would case a *PHE* (*PPHE*):

$$PPHE = \frac{2 \times PHEI}{48hr} \quad (9)$$

It is not trivial to define what values should be used for *PL* and *MD*. To be conservative, in our simulations we used the maximum SV observation gap at each location (the lapse of time an SV is not seen from the LGF), and the minimum maneuver time (based on all maneuvers for the year 2004) [9]. A map of the resulting *PPHE* values worldwide can be observed in figure 2. From the values on that plot we can say that only 35% of the total exposure time a maneuver can actually lead to a *PHE*. We will conservatively assume there are 18 SVs in view at each epoch. We are now ready to assign a value to $P[A]$:

$$\begin{aligned} P[A] &= OR_f \times ET_f \times 18 \\ &\quad + OR_M \times (ET_M \times PPHE) \times 18 \\ &= 1.27 \times 10^{-5} \times 2 \times 18 + 2 \times (\frac{2}{365} \times 0.35) \times 18 \\ &= 4.57 \times 10^{-4} + 0.069 \end{aligned} \quad (10)$$

We now have all the elements to determine what value needs to be assigned to (6) to meet the integrity requirement for A1 ephemeris threat mitigation. From (2) (3) (4) (5) and (10):

$$\begin{aligned} P[MN] &\le \frac{P_{A1HMI}}{P[A] \times P[B] \times P[D]} \\ &= \frac{2.07 \times 10^{-8}}{0.0695 \times 1.27 \times 10^{-5} \times 1} = 0.0235 \end{aligned} \quad (11)$$

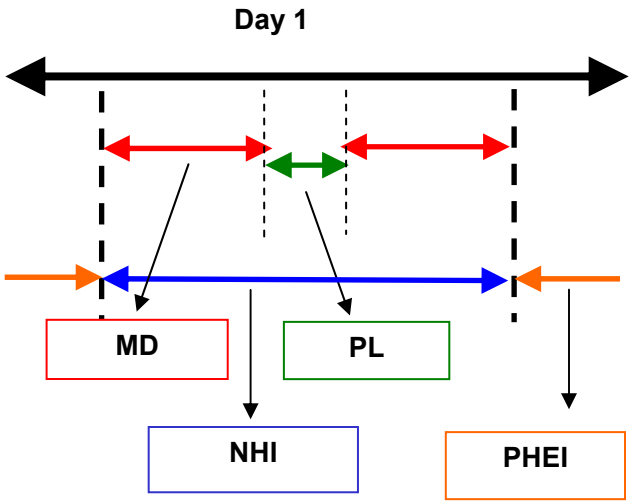


Figure 1: Potentially Hazardous Event Intervals

We will now asses the impact of the *FR* on the ephemeris monitors.

For the Type B monitor, as $1.27\times10^{-5} < 10^{-4}$, the analysis done in previous work is conservativ regarding the *FR*.

For the A1 monitor, the requirement is reduced to a P[*MN*] < 0.0235. This is equivalent to saying that for each *PHE* that is detected by the OCS (and we have concluded that within 2 hours all of them are), the OCS can fail to notify, and/or the LGF fail to receive the notification 1/*P*[*MN*] times, that is, one out of 43 times. We will address the possible notification channels in the next section.

In case the required *P*[*MN*] can be met, then all ephemeris failure types would be mitigated. We have shown evidence for Type B (studies done before this paper are backed up by *FR* derived in this work) and Type A1 failure (also from *FR* but with new requirement for *MN*). This conclusion is also true for the Type A2 failures, as all maneuvers would have a previous warning through a NANU, and maneuvers coming from a spontaneous firing of a thruster that lead to a large orbit error are considered to have a negligible probability of occurrence.

It is worth noting that if this new requirement on notification had not arisen from the analysis (meaning the only *PHE* considered is a failure, not including any planned maneuver), the elimination of an A1 monitor would have been justified, given that, even without assigning any detection capabilities to the LGF or the OCS the *P*[*A*] would only include the first term in (10):

$$P[A]\times P[C]=4.57\times10^{-4}\times1.27\times10^{-5}=5.8\times10^{-9}<P_{A1HMI} \quad (12)$$

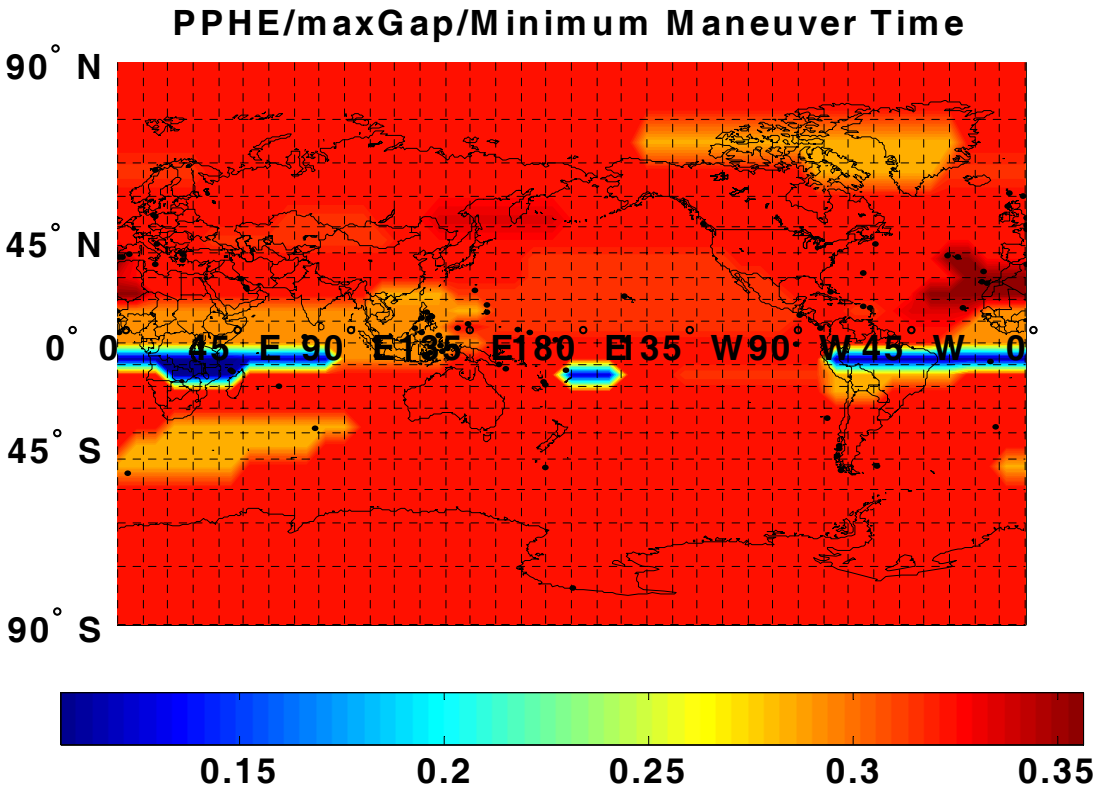


Figure 2: Percentage of time a maneuver will be a Potencially Hazadous Event (PPHE)

## MISSED NOTIFICATION

Several notification channels were considered for the LGF to learn of a *PHE* after it is detected (or scheduled in case of a maneuver) by the OCS:

SV message Health status: This channel is not reliable, as a failure could exist while the SV is in view on days 1 or 2, but OCS detection could occur when it is no longer in view, or a maneuver could happen out of view. Then the LGF would never see the 'UNHEALTHY' message.

Almanac Health status from any SV's message: This is also not reliable, as the almanac is provided for fast localization of SVs in the sky, and not for integrity or navigation purposes [4][10]. (A change of health status on a satellite does not necessarily imply an upload to update the almanacs.) Almanacs are guarantied by ICD-200 to not be older than 6 days [10], so maneuvers are likely to be included in almanac, but no assurance is provided.

NANUs: Notice Advisory to Navstar Users. It is the official constellation change notification method. NANUs are issued by the Air Force, and transmitted to civil users by the Coast Guard. For maneuvers, 48 hour advance notice is provided (72 hr in the last few years), for non-scheduled events notification is provided "as soon as possible after the event". The notification from the Coast Guard is done through the internet. [9]

Then, the key is to find a way at the LGF of receiving NANUs that is reliable enough as to not miss more than one out of 43 NANUs informing of a maneuver. With respect to planned maneuvers the analysis is simpler, as "missing" the notification implies not receiving it for at least 48 hr, and the Coast Guard not only has the NANUs but also a constantly updated summary of NANUs that are 'live', (that is, all NANUs containing information warning of a future activity, or informing of a particular issue about an SV for which it cannot be used or will not be available for use in the future).[9] This means that even if the NANU was missed when the initial notification occurs, there is a period of at least 48 hr to check the NANU satus summary. For non planned maneuvers, a more detailed study is needed to asses their frequency, and how rapidly they are informed of.

The reliability of internet connectivity also has to be studied to establish the feasibility of implementing this simplified 'NANU checking' A1 monitor. This includes the possibility of some LGF not having access to the internet at all which would preclude this monitor as an option.

As the necessary studies to establish if checking NANUs is a reliable option have not been executed, and it would always be desirable to have a system that does not depend on any communication channel outside the LAAS system, some options for monitoring the threats that remain unmitigated are presented at the end of the paper.

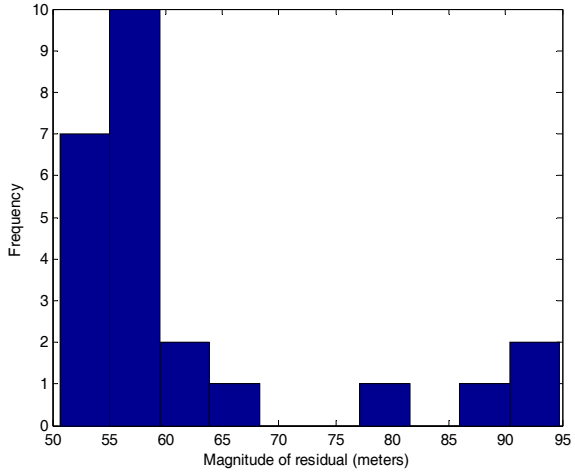


Figure 3: Magnitude of SV position discrepancies

## FAILURE RATE FROM DATA

When deriving the *FR*, great care was taken in making only assumptions that were considered conservative. However since there is no official source addressing the *FR* directly, and assertions not included in the official documents were used, we feel it is necessary to verify the obtained value by observing the historical ephemerides.
The general procedure is comparing the 'true' position of the satellite with the position generated from the broadcast ephemeris. If the two positions agree, the ephemeris is considered correct, if the position error exceeds a certain predetermined threshold, it is a potential ephemeris failure. The 'true' SV position is obtained from the International Geodetic Survey (IGS) which stores SV positions every 15 minutes. This data is based on orbit determination using post proceesed measurements observed at various ground facilities, and the precision is about 5 to 10 meters, which is enough for our purposes [11]. The ephemerides are obtained from The NASA Crustal Dynamics Data Information System (CDDIS) when available, as it has all ephemerides for all SV's. When the ephemerides were not available (basically before the year 2000) the ephemerides were extracted from the University of California San Diego Scripps Orbit and Permanent Array Center (UCSD SOPAC) database. This is available on a per site basis, so different sites have to be looked at to obtain all the ephemerides. There were several storage errors detected that were solved by cross checking different sources. Also some isolated data points were missing from the IGS or the ephemeris storage sources, but it is reasonable to say a comprehensive coverage of a whole decade (1997-2006) was performed

for all SV's in the sky at each time, and all ephemerides transmitted.

An initial set of discrepancies > 50 m was obtained, and for each one of them, the archived NANUs were checked to see if there was a warning or a planned maneuver at that time. After eliminating all cases included in outage times (from NANUs prior to the discrepancy time), only 24 cases remained, all with magnitudes smaller than 100 m (figure 3).

It is difficult to prove that these cases were not failures, as the storage interval at the IGS is 15 minutes, and since we cannot know at what time the SV started broadcasting an 'UNHEALTY' signal, it is impossible to know exactly when this error was detected and corrected by the OCS. However, ephemeris errors of 100 m are not considered to be a major threat for LAAS[8]. In other words, we cannot prove these 24 cases are not failures, but even if they were, their magnitude indicates they are not a major threat to LAAS navigation.

We will try to determine what these values mean in terms of the confidence level for our derived *FR*. Given a failure rate *fr* and a number of samples *S*, the probability of a certain number of failures *k* happening can be approximated accurately with a Poisson distribution function [12] as:

$$P(k) = \frac{(fr \times S)^k \times e^{-(fr \times S)}}{k!} \qquad (13)$$

The probability of *k* or less cases is given by:

$$P(k \text{ or less}) = \sum_{l=0}^{k-1} P(l) \qquad (14)$$

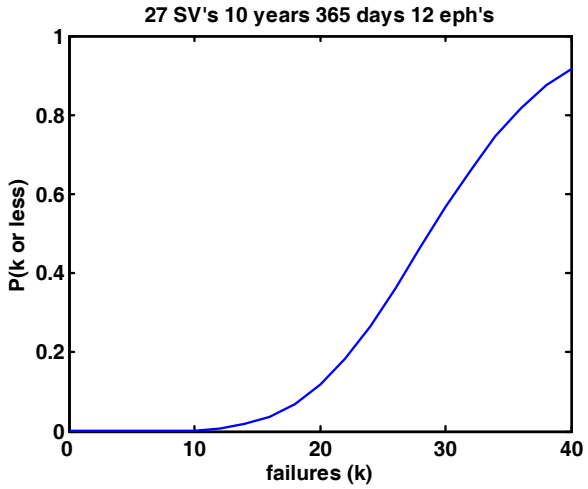


Figure 4: Confidence for different number of failures

If we make *fr=2×FR* (note that when we derived *FR* we only considered the failures 'in sight' of a particular LGF, and now we are looking at all potential failures), and *S*= the number of ephemerides for 10 years, we can plot the value in (14) for different *k* 's (figure 4)

If we consider all discrepancies smaller than 100 m as non-failures, then *k*=0. We can see in the plot that the confidence level (in percentage: 1 minus the value on the y axis multiplied by 100) is almost 100%. If we consider the episode of April 2007, the confidence level is still close to 100 %. Even if we considered all the cases above 50 m (24 cases) the confidence level would still be above 75%. We consider this to be a strong indication that the *FR* being used in this work is conservative.

## UNMITIGATED THREATS

As was stated before, if the LGF has a way of reliably checking NANUs (not missing more than one in 43), all threats would be covered. If this NANU checking system cannot be implemented, then three other cases remain unmitigated:

1) An ephemeris failure detected by the OCS, but whose notification is not received at the LGF. This would basically be the case of the last ephemeris before setting, that might not be in view the full two hours. In this case the LGF might not see the 'UNHEALTHY' message after detection from the OCS.
2) A planned maneuver that happens out of view of the LGF
3) A planned maneuver in view of the LGF, where the health bit is not changed to 'UNHEALTHY' by the OCS (event of April 10th)

The first case seems to be the easiest to solve, as a Zero Order Hold (ZOH) test could be applied using the immediately previous ephemeris to validate the last ephemeris of the day (this 2 hour ZOH has much better results than the 24 hours FOH test executed by the Type B monitor).[13]

The other two cases could be mitigated at the LGF with two tests that are very easy to implement: a Range Test (RT), and a Range Rate Test (RRT). These tests will compare the expected range and range rate (using the ephemeris to be validated), with the range and range rate measured at the LGF (that will include the effect of a maneuver if it took place). As the two last unmitigated cases relate to planned maneuvers, there are some assumptions that can be made about the direction and ΔV of the maneuver. It can be assumed that all maneuvers will be done mainly within the satellite's orbit plane, and within a range of a certain change of velocity. This constraint on the types of possible maneuvers allows us to

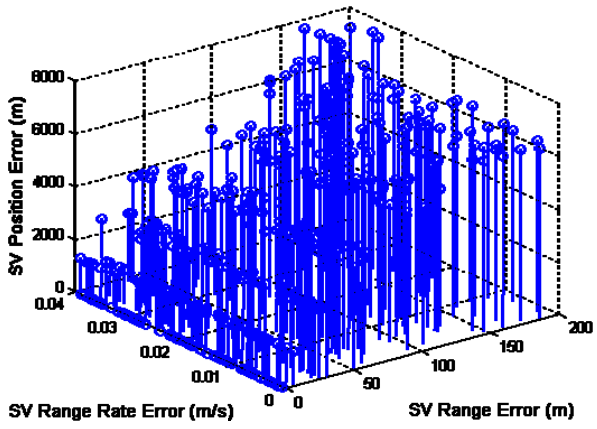


Figure 5: SV position errors and RT and RRT values

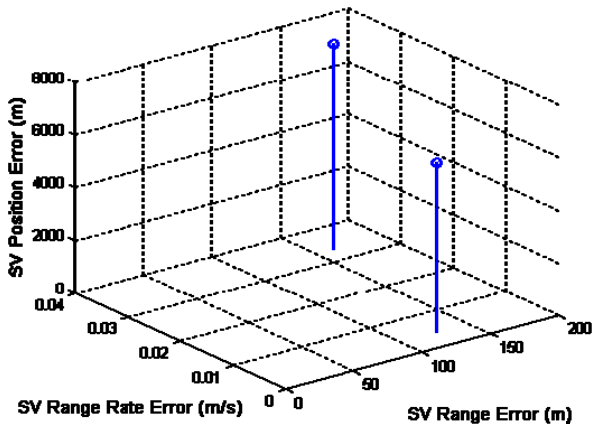


Figure 6: Undetected PHE (maneuvers)

simulate how much the SV position deviates from the pre-maneuver orbit at different times after the maneuver. In parallel we can analyze the LGF Line Of Sight (LOS) range and range rate differences (also relative to the premaneuver value). These LOS components are the ones observed by the RT and RRT monitors respectively. We will assume RT and RRT thresholds of 100 m and 0.02 m/s respectively as they will yield negligible false alarm rates. We will assume that the monitor might be 'seeing' a nominal error equal to the threshold value and in the opposite direction of the positon or rate error caused by the maneuver. Accordingly, in the analysis we will not take credit for detection unless the range or range rate discrepancy is twice as big as the threshold (200 m and 0.04 m/s respectively). Taking into account the magnitudes of an ephemeris error that can be hazardous for a Cat I LAAS user [1], we will consider any (undetected) SV position error bigger than 2500 m as a possible *HMI*.

In our initial analysis, the maximum possible maneuver $\Delta V$ is assumed to be 10.8 m/s [7], and completely in the intrack direction. A preliminary study suggests that 7 m/s is the worst maneuver size (because large SV postion errors can result, but the range and range rate errors are not as large as they would be for $\Delta V$ = 10.8 m/s), and all results shown in this section correspond to this value of $\Delta V$. To simplify the simulations, we assume LGF locations at different latitudes along one meridian, and one satellite orbit plane whose ascending node will be rotated 360 degrees. For each position of the node, the starting maneuver point is moved within the plane through 360 degrees. The satellite position error is computed for each maneuver starting point, and then the range and range rate discrepancies are evaluated as they would be seen from each LGF in the chosen meridian. This way all possible GPS constellations, user locations and burn times are covered. The spacing for LGFs, ascending nodes and mean anomaly maneuver starting point is one degree for all cases. The results for all these cases, as well as the impact of spacing changes on them are still being evaluated

We present here some preliminary numbers for one site (Memphis) using the nominal DO-229 24 SV constellation[14]. Figure 5 shows all the epochs for which the SV position error is bigger than 2500 m and both the RT and the RRT components caused by the maneuver are smaller than twice the respective thresholds. However, some of these cases might not be real situations of *HMI*. If either monitor sounds the alarm before the SV position error reaches 2500 m, then the hazardous event never takes place. In that case the alarm will make the LGF stop broadcasting corrections for that SV, and the two day wait for the Type B monitor will start. We can then eliminate as *PHEs* all cases for which one of the two alarms sound (when the range deviation is bigger than 200m, or the range rate deviation is bigger than 0.04 m/s) at any moment between the time the monitors start checking the satellite (5 degree elevation) and the moment the SV reaches a position deviation from the nominal orbit bigger than 2500 m. The remaining cases are shown in figure 6.

We can eliminate even more cases by starting the monitors before the mask of 5 degrees. In the example considered, the remaining cases shown in figure 6 would also be detected if the monitor is started at 3 degrees. [Note: The LGF would still wait until the SV reaches the 5 degree mask to broadcast corrections for that satellite, but the monitors will be functioning from the moment the SV reaches 3 degrees].

These initial results show that the range monitor and the range rate monitor might effectively provide integrity for *PHE* resulting from maneuvers.

## CONCLUSSIONS

This work derives an ephemeris Failure Rate *FR* from the GPSSPSPS document. The conservative nature of the obtained *FR* is confirmed by analyzing 10 years of stored ephemerides in search of failures. The impact of applying this value in the analysis of the different ephemeris threats that can affect LAAS is demonstrated, showing it is sufficiently small to support the Type B monitor, as well as to eliminate the need of a Type A monitor as it was originally designed. However a new requirement on the Probability of Missed Notification is derived. In order to meet this requirement the LGF should be able to check NANU's with a missed message rate of not more than one out of every 43 that are issued. In case this requirement cannot be satisfied at the LGF, alternative monitor ideas are presented to mitigate the remaining threats: basically a zero order hold test on the last ephemeris before an SV sets, and range and range rate monitors to detect maneuvers that the LGF is unaware of. Analysis of the effectiveness of these monitors is still in progress, but initial results are promising.

## ACKNOWLEDGMENTS

The authors want to thank Karl Kovach for patiently answering our questions about the OCS standard procedures, and Jim Slater for providing information regarding the spatial gaps in SV monitors from the ground for GPS.

## REFERENCES

[1] Gratton, L.; et.al; Orbit Ephemeris Monitors for Category I LAAS", Proceeding of the IEEE Position, Location, and Navigation Symposium, PLANS '2004, Monterey, CA, April 2004

[2] Gratton, L., et.al, "Experimental Observations and Ephemeris Monitor Applications of LAAS Carrier Phase IMLA Measurements", Institute of Navigation's GNSS meeting, Long Beach, CA, September 2004

[3] Federal Aviation Administration GPS Product Team, "Global Positioning System Standard Positioning Service Performance Analysis Report" Report #58, June 31st 2007

[4] Global Positioning System Standard Positioning Service Performance Standard, Department of Defense, October 2001

[5] Private conversation with Jim Slater, March 2007

[6] Creel, T., et.al. "The Legacy Accuracy Improvement Initiative", GPS World, March 2006

[7] Private conversation with Karl Kovach, May 2007

[8] Pervan, B.; et al. "Ephemeris A1 Monitor", Breifing to the FFA, February 27th 2007

[9] GPS Advisories/NANUs, Coast Guard Navigation Center Website

[10] ICD-200, "Navstar GPS Segment/Navigation Users Interfaces", September 27th 1997

[11] "Data and Components, igscb", National Aeronoautics and Space Administration, Jet Propulsion Laboratory website.

[12] Salkind, N; Binomial Distribution: Encyclopedia of measurements and Statistics, Thousend Oaks, Ca, 2007

[13] Gratton, L., "Orbit Ephemeris Monitors for Category I Local Area Augmentation of GPS" M.S. Thesis, Dept. Of Mechanical, Materials, and Aerospace Engineering, Illinois Institute of Technology, Chicago, July 2003

[14] SC-159 RTCA "Minimum Operational Performance Standards for the Global Positioning System/Wide Area Augmentation System Airborne Equipment", DO-229, December 13th 2006