Bayesian Inference of GNSS Failures

Carl Milner, Christophe Macabiau, Paul Thevenon

Bayesian Inference of GNSS Failures

Carl Milner, Christophe Macabiau, Paul Thevenon
Ecole Nationale de l'Aviation Civile
milner@recherche.enac.fr

ABSTRACT

The *probability of failure* (*failure rate*) is a key input parameter to integrity monitoring systems used for safety, liability or mission critical applications. A standard approach in the design of Global Positioning System (GPS) integrity monitoring is to utilize the service commitment on the probability of major service failure, often by applying a conservative factor. This paper addresses the question of what factor is appropriate by applying Bayesian inference to real and hypothetical fault histories.

Global Navigation Satellite System (GNSS) anomalies include clock or signal transmission type faults which are punctual (may occur at any time) and incorrect ephemeris data which are broadcast for a nominal two hours. These two types of anomaly, classified as *continuous* and *discrete* respectively are addressed. Bounds on the total probability of failure are obtained with given confidence levels subject to well defined hypotheses relating past to future performance. Factors for the GPS service commitment of 10^{-5} per hour per satellite are obtained within the range two to five with high confidence (up to $1\text{-}10^{-9}$).

KEYWORDS: Integrity, GNSS Vulnerability, Failure Modes and Effects Analysis, Bayesian

1. INTRODUCTION

The Global Navigation Satellite System (GNSS) *failure rate* is a key parameter in the design of safety, liability or mission critical applications. At present, only the Global Positioning System (GPS) publishes a Performance Standard (PS) for civilian use which includes service commitments relating to this probability (GPS, 2008). The commitment of 10^{-5} per hour per satellite, translates to about 3 per year over the entire constellation (GPS, 2001). This value is based on a blend of experience obtained from past failure events (Van Dyke et. al*., 2003*; Van Dyke et. al., 2004) and reliability analysis undertaken for the constellation and ground segment.

The use of GNSS within the safety critical domain of civil aviation has led to many integrity monitoring developments. Placing trust within the service commitments provided by GNSS Service Providers (GSPs) represents an external risk to aviation certification authorities whose primary role it is to maintain the safety of passengers and crews within its airspace. To meet aviation's strict requirements, a number of approaches have been undertaken to lessen the external risk of the certification authority.

These solutions or *augmentations* are the Satellite Based Augmentation System (SBAS), the Ground Based Augmentation System (GBAS) and the Aircraft Based Augmentation System (ABAS) (ICAO, 2006). The latter includes the class of consistency checking algorithms known as

Receiver Autonomous Integrity Monitoring (RAIM). SBAS is built on dense regional networks of stations incorporating fault monitors which place very little trust in the core GNSS. GBAS utilizes local reference stations with monitors whose performance is based on equally conservative prior probabilities of fault occurrence. In fact, the U.S GBAS implementation known as LAAS assumes 10^{-4} per hour per satellite, ten times that of the service commitment (Pullen et. al., 2006).

Integrity Monitoring techniques are often founded on equating the *integrity risk* for a failure to the product of the probability of occurrence of the failure, often expressed in the range domain, and the probability of missed detection, expressed in the position domain and defined as the event of the positioning error e exceeding the alert limit AL and the monitoring test statistic T not exceeding the threshold T_h (Lee and Van Dyke, 2002).

$$\boldsymbol{IR = P_{fail} \times P_{md}(e > AL | T < T_h)} \quad (1)$$

The total integrity risk is then predicated on summing mutually exclusive failure cases. The RAIM methodology employed in ABAS (Lee and Van Dyke, 2002; RTCA, 2004), is inherently founded on a satellite fault probability of 10^{-5} per hour (Pullen et. al., 2006; Lee and Van Dyke, 2002).

Future architectures are being assessed within the aviation community which aim to provide the relative autonomy and low costs of RAIM without the need to place significant trust in the core GNSS (FAA, 2010; Blanch et. al. 2013). One such architecture, Advanced RAIM (ARAIM), is the subject of the Working Group C ARAIM Technical subgroup (ARAIM SG) (Blanch et. al., 2013; WG-C, 2012). Discussion within the ARAIM SG has focused on the question of *how much trust can be placed in the core GNSS?* This paper proposes a solution to the associated question of *how do we quantify the trust we place in the core GNSS?*

The methodology presented is applicable to any safety, liability or mission critical GNSS application that places trust in the core GNSS. The alternative is to assume that all GNSS fault modes occur with a probability of unity as taken for the ionosphere threat to CAT II/III GBAS (Murphy et. al., 2010).

The paper is organized as follows. Section 2 presents the available methodologies. Section 3 presents the failure types and partitions them for the appropriate analysis of sections 6 and 8. Section 4 introduces the failure rate model. Section 5 presents the Bayesian inference methodology. Section 6 applies Bayesian inference to the observed continuous time fault history. Section 7 presents the application to new satellite blocks. Section 8 addresses discrete time failures. Section 9 presents the combined failure model including an algorithmic framework outlining the role of the preceding sections before Section 10 concludes.

2. FOUNDATIONS

This paper determines the probability of failure onset without accounting for the transition from a fault mode to the fault-free mode following control segment intervention (GPS, 2008; Blanch, 2012). A number of different approaches may be taken as outlined below.

2.1 Acceptance of the Performance Standard

A first approach could be to accept the standards provided by the core GNSS such as in the GPS Standard Positioning Service (SPS) Performance Standard (PS) (GPS, 2008) and the associated external risk. The GPS SPS PS defines a *Major Service Failure (MSF)* to occur when the Instantaneous User Ranging Error (IURE) exceeds 4.42 times the satellite's broadcast User Ranging Accuracy (URA). The standard then states that an MSF will not occur with a probability greater than 10^{-5} per hour per satellite which equates to approximately three failures per year over the constellation. The URA is broadcast for each satellite and varies with time, as does the true distribution of the IURE, whereas from the user perspective, a ranging failure, which may lead to a positioning failure, depends upon the time-varying user-satellite geometry. Furthermore, the *MSF* magnitude could potentially be larger than the failures which must be addressed, to support, say LPV-200 operations with ARAIM (ICAO, 2006; FAA, 2010; WG-C, 2012).

2.2 Fault Tree Analysis

Alternatively, fault tree analysis could be applied within a risk assessment of the core GNSS space and ground segments. A Failure Modes and Effects Analysis (FMEA) is performed, capturing the faults with the potential to cause a positioning failure (Van Dyke, 2003; Van Dyke et. al., 2004). Table 1 presents the list of feared events considered for ARAIM (WG-C, 2012). The advantage of this approach is setting very low probabilities to rare faults with sufficient justification. However, there is a tendency to conservatively but arbitrarily inflate the prior probabilities of other failure events, thus negating the gains.

2.3 Empirical Approach

The approach taken in this paper is to estimate the failure rate for the ensemble of feared events using the fault history. It is a methodology readily available to the navigation community given the extensive data stored globally and thus enables the use of data mining activities to capture the occurrence of failure events (Heng et. al., 2010). Previous fault analyses employed within the augmentation system definitions have assumed failure rates for different feared events based on an analytical expert opinion, to which conservative factors are then applied (Shively, 1999).

3. FAILURES AND FEARED EVENTS

The approach taken in this paper is based on the true unknown time-varying satellite failure rate λ. In order to fully understand its properties, the following failure definitions are considered:

- *Ranging/Positioning Failure:*
  the event that the instantaneous error (range or position domain) exceeds a predefined threshold (Figure 1 & Figure 2) (GPS, 2008).
- *Integrity Failure:*
  the event that the probability of an instantaneous position error exceeding a predefined threshold without timely detection, exceeds a predefined probability limit (Figure 3) (ICAO, 2006)
- *Overbounding Failure:*
  the frequency density which lies outside the assumed model (Figure 4) (DeCleene, 2000)
- *Statistical Failure:*

a change in the underlying error distribution to a 'failure' state defined by statistical parameters (i.e. mean and sigma) (Figure 5) (Lee et. al., 2006)

These definitions may be applied in the range domain, position domain or test statistic domain (Sturza, 1989). Whilst the performance commitments are naturally in the range domain (GPS, 2008), the position domain is used for the application requirements (ICAO, 2006).

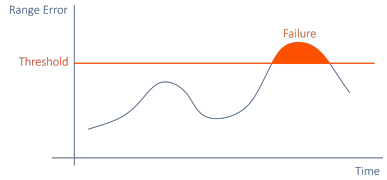

Figure 1: Range Error Failure

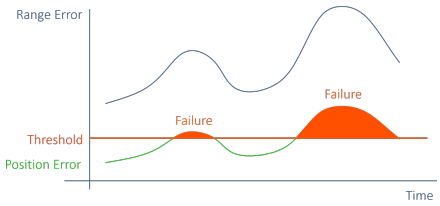

Figure 2: Positioning Failure

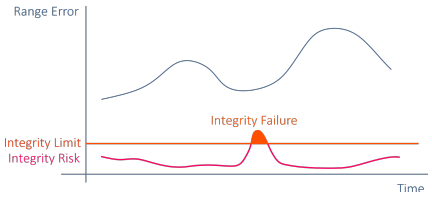

Figure 3 Integrity Failure

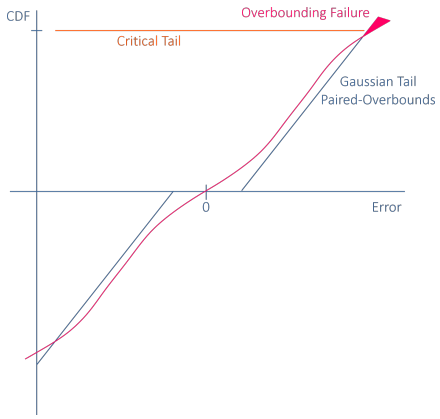

Figure 4: Overbounding Failure

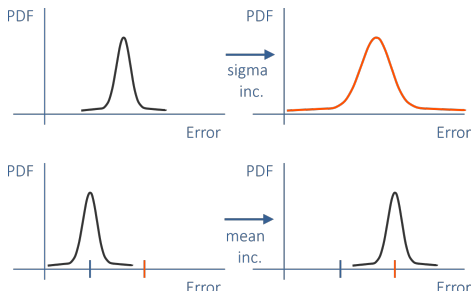

Figure 5: Statistical Modelling Failure

Navigation system requirements are expressed in terms of either positioning failures or integrity failures (ICAO, 2006), yet implicit assumptions are made that the mathematical techniques employed and the physical assumptions taken are valid. This provides the link between the natural definitions of Figure 2 and Figure 3 with those of Figure 4 and Figure 5. The *MSF* event (GPS, 2008) is a function of URA. However, when the IURE remains below the $4.42 \times URA$ value, a change in the underlying error distribution, such as an increased mean or inflated standard deviation can also represent a *failure* condition. This is the case if the zero-mean Gaussian model parameterised by URA no longer overbounds the true distribution.

In this paper, the range failure of Figure 1 is taken as the baseline. Whilst, such events may be understood to occur at the onset of the defined failure windows shown in Figure 1, Figure 2 and Figure 3, it is not immediately obvious how a rate can be applied to the failure interpretations expressed by Figure 4 and Figure 5.

Table 1 lists the most commonly considered feared events (WG-C, 2012). Column three codifies whether the fault occurs at a punctual *continuous* (and random) point in time (C) or during a *discrete sample* with correlation throughout the sample period (typically two hours) (D). These cases are handled separately in sections 5-6 and 8 respectively. Nominal events consisting of both types are denoted (B).

Table 1: Feared Events

Feared Event	Comment	C/D
Nominal Clock + Ephemeris Error	Incorrect overbounding/statistical modelling by the URA	B
Single Fault Clock and Ephemeris Fault - *Physical*	Physical satellite clock run-off / excessive acceleration or uninformed manoeuvre / thruster firing	C
Single Fault Clock and Ephemeris Fault - *Message*	Upload of incorrect ephemeris and clock offset model parameters. Correlated in time throughout the period of navigation message transmission (nominally up to two hours)	D
Wide Clock and Ephemeris Fault - *Physical*	Physical satellite clock run-off / excessive acceleration or uninformed manoeuvre / thruster firing on multiple satellites	C
Wide Clock and Ephemeris Fault - *Message*	Upload of incorrect ephemeris and clock offset model parameters. Correlated in time throughout the period of navigation message transmission (nominally up to two hours)	D
Nominal Signal Deformation	Incorrect overbounding/modelling through the URA and ICAO signal deformation modelling	B
Single Fault Signal Deformation	Physical ‘evil waveform’ event can occur at any continuous time	C

Nominal code-carrier incoherence	Incorrect overbounding/statistical modelling by the URA.	B
Single Fault code-carrier incoherence	Physical effect of divergence between the code and carrier phases as a result of payload failure	C
Nominal IFB	Incorrect overbounding/statistical modelling through the broadcast IFBs and URA.	B
Single Fault IFB	Physical effect of the divergence between the frequency delays at the satellite hardware	B
Nominal Antenna bias	Incorrect overbounding/statistical modelling by the URA (satellite hardware effects) and user receiver model sigma	C
Single Fault Antenna bias	Physical effect of a hardware failure.	C
Nominal Ionospheric error	Not considered – addressed by ionosphere free smoothing	C
Single Fault Ionosphere	Not considered – addressed by ionosphere free smoothing (Pullen et. al., 2006)	C
Wide Fault Ionosphere	Not considered – addressed by ionosphere free smoothing	C
Nominal Tropospheric error	Not considered – relates to overbounding/statistical modelling failure of the troposphere model	C
Single Fault Troposphere	Not considered – see (van Graas and Zhu, 2011)	C
Nominal Code Noise and Multipath	Not considered – user segment fault	C
Receiver Fault	Not considered – user segment fault	C

A *failure (condition)* as defined by Figures 1 to 5 is distinguished from a *fault* being the physical event (payload functioning in an abnormal state). The table of feared events presents both faults and other events which may occur nominally and lead to a *failure condition*. In that regard a *feared event* is a type of *fault*.

The rate λ does not include failures due to the signal environment or user segment equipment. The probability of space and control segment failures depends upon the satellite's hardware (clock age, payload, block design) or the ground control segment (network, software, operational status). This variability of the failure rate λ as a function of time is addressed in the following section.

4. FAILURE RATE MODEL

This paper presents a *Bayesian* approach to determining the true failure rate (O'Hagan and Forster, 2003). It is assumed that the physical process's true failure rate exists and may be estimated using Bayesian analysis as opposed to a classical approach (Neyman, 1937). Whilst a confidence distribution may be constructed by extending the classical notion of the confidence interval, such an approach has not been extensively formalised (Fraser, 2011). The advantages of a Bayesian approach are that it allows a more natural means to express the *posterior* distribution for the estimated random parameter. Furthermore, understanding this parameter to be time-varying and random allows an easier interpretation of the conditions in which the approach is valid (as expressed in hypotheses 1-3). Finally, whilst this paper ultimately selects a non-informative prior, the Bayesian approach maintains the possibility of combining the technique with prior information from an FMEA.

Following this Bayesian approach, initially the mathematical formulation is restricted to punctual, continuous time events. If the true instantaneous failure rate is known to be constant then the

number of failures observed over a given duration would follow a Poisson process (Cox and Isham, 1980). Due to changes in the control segment, the active satellite clock and aging of payload components, the true instantaneous *failure rate* varies with time. The Non-Homogeneous Poisson Process (NHPP) with variable failure rate $\lambda(t)$ models this real system (Pham, 2006). Under the NHPP the true expected number of failure events up to time T is:

$$\boldsymbol{m(T) = \int_0^T \lambda(t)\, dt} \tag{2}$$

The probability of k failures having occurred over the period $[0, T]$ is then known to follow the standard Poisson relation:

$$\boldsymbol{P(k) = \frac{m(T)^k}{k!} e^{-m(T)}} \tag{3}$$

To utilise this result in the future, the following two hypotheses are assumed:

H1. Short term variations in $\lambda(t)$ are not observable

H2. $\forall T\ \exists S > T\ s.t\ \ \frac{m(T)}{T} \geq \frac{\int_0^S \lambda(t)dt}{S}$

Hypothesis 1 states that whilst the system changes from ground operational actions, satellite aging and other factors, the impact on the instantaneous probability of failure cannot be determined from data. It is a *hidden variables* statement that supposes all that is undeterminable may be considered random. What is of interest is the likelihood that the number of failure events exceeds the number that is predicted.

Aircraft perform approach and landing operations using monitoring algorithms predicated on a particular failure probability. If the true failure probability exceeds this value during an approach but this value is not determinable as the fluctuations from causal relations are too complex to determine, it is then appropriate to assert that the system meets the integrity requirements based on the best available knowledge. The alternative is to estimate the impact of satellite aging and all other factors upon the failure rate. However, the authors' view is that this is too complex to model appropriately.

Hypothesis 2 goes further by relating the expected failure rate at time T to future expectations of the failure rate. It states that a future time S exists where the true expected failure rate will be no greater than the current expected rate. It may be understood that the total system reliability does not degrade over the long term. Note this hypothesis applies to the total system rather than a particular satellite. It asserts that *a* future time S may be found, and *not* that the condition holds for *all* S.

The service commitment may then be understood as implementing *sound processes*, by maintaining the same rigour in satellite and ground system design, mitigating observed problems in the control segment operations and maintaining satellites as they age. The variable $\boldsymbol{\lambda}$ is then used as the true mean failure rate $\lambda = m(t)/T$ which for the purposes of notational simplicity is scaled to be the rate per T (to be rescaled when expressing the results per hour as in Table 4) and the model reduces to the Poisson Process (Cox and Isham, 2006).

$$\boldsymbol{P(k) = \frac{\lambda^k}{k!} e^{-\lambda}} \tag{4}$$

5. BAYESIAN INFERENCE

Inference may be made using past failure data to estimate the posterior distribution of λ. Bayes theorem for a continuous variable λ with discrete events k is as follows (Box and Tiao, 1973):

$$\boldsymbol{f(\lambda|k) = \frac{P(k|\lambda) f(\lambda)}{\int P(k|\lambda) f(\lambda)\, d\lambda}} \tag{5}$$

where:

$P(k|\lambda)$ - probability of k failure events occuring over T given λ

$f(\lambda)$ - continuous prior PDF for λ

$f(\lambda|k)$ - continuous posterior PDF for λ

The quantity of interest is the continuous posterior distribution for the failure rate $f(\lambda|k)$. Over a given period with a given definition of failure, k may be determined. The Poisson model determines the values the function $P(k|\lambda)$ takes whilst the prior probability $f(\lambda)$ may be formed using two approaches (Box and Tiao, 1973; Jeffreys, 1946):

A. *Non-informative* reference priors giving the data maximum weight over prior information

B. Priors expressed using standard conjugates based on '*expert opinion'*

For completeness, both approaches are used to check whether the choice of prior has a strong impact on the results. The form of the conjugate prior distribution does not influence the inference output significantly, what is critical are the CDF percentiles.

Firstly, the conjugate distribution to the Poisson distribution which may be used for the prior $f(\lambda)$, the *Gamma* distribution, is introduced (Raiffa and Schlaifer, 1961):

$$\boldsymbol{f(\lambda) = \frac{\alpha^{\nu} \lambda^{\nu-1} e^{-\alpha\lambda}}{\Gamma(\nu)}} \tag{6}$$

with shape parameter ν, scale parameter $1/\alpha$, and the gamma function $\Gamma(\cdot)$

Three reference priors are employed (Box and Tiao, 1973; Jeffreys, 1946) :

Bayes Uniform Prior: ($\nu = 1$ & $\alpha = 0$)

$$\boldsymbol{f(\lambda)} \propto \begin{cases} \mathbf{1/M} & \mathbf{0 \leq \lambda \leq M} \\ \mathbf{0} & \mathbf{otherwise} \end{cases} \text{ where } \boldsymbol{M \to \infty} \tag{7}$$

Albert's Prior: ($\nu = 0$ & $\alpha = 0$)

$$\boldsymbol{f(\lambda)} \propto \frac{\mathbf{1}}{\boldsymbol{\lambda}} \tag{8}$$

Jeffrey's Prior ($\nu = 1/2$ & $\alpha = 0$):

$$\boldsymbol{f(\lambda)} \propto \frac{\mathbf{1}}{\sqrt{\boldsymbol{\lambda}}} \tag{9}$$

Although there is no single standard reference prior, *Jeffrey's prior* is the most commonly employed.

In addition, hypothetical expert opinions are considered, expressed in terms of the conjugate prior. The gamma distribution parameters and percentiles are given in Table 2, selected with respect to the GPS constellation.

Table 2 Expert Opinion Conjugate Priors

Expert Opinion	ν	α	Mean/year	95%/year	Comments
Positive	3	0.1	1.5	3	95% at 3/year
Realistic	3	0.05	3	6	Mean at 3/year
Conservative	2.5	0.02	6.25	14	95% at 1/month
Highly - Conservative	2	0.005	67	47	5% at 3/year 95% at 1/week

The *positive* expert in the first row of Table 2 is the expert opinion of following the recent trend. The *realistic* expert view follows GPS SPS PS (2008) whilst the *conservative* view holds a 95% confidence that a fault per month is to be expected and the *highly conservative* a 95% confidence of a fault per week. Table 3 presents the respective Gamma distribution parameters.

Table 3. Prior Distribution Parameters

ID	Prior	2ν	2α
1	Uniform	2	0
2	Albert	0	0

3	Jeffrey	1	0
4	Positive	6	0.2
5	Realistic	6	0.1
6	Conservative	5	0.04
7	Highly Conservative	4	0.01

Employing the parameters given in Table 3 gives the following posterior distributions:

1 $$f(\lambda|k,0,1\ ) = \frac{e^{-\lambda}\lambda^{k}}{\Gamma(k+1)}$$

2 $$f(\lambda|k,0,0) = \frac{e^{-\lambda}\lambda^{k-1}}{\Gamma(k)}$$

3 $$f\left(\lambda|k,0,\tfrac{1}{2}\right) = \frac{e^{-\lambda}\lambda^{k-\frac{1}{2}}}{\Gamma\left(k+\frac{1}{2}\right)}$$

4-7 $$f(\lambda|k,\alpha,\nu) = \frac{e^{-(1+\alpha)\lambda}\lambda^{k+\nu-1}(1+\alpha)^{k+\nu}}{\Gamma(k+\nu)}$$

Integrating the posterior distributions with a k value taken from the fault history determines the true failure rate with a given level of confidence. Example results are given in the appendix for various k values and show only minor differences. The exception is for a low k value (Table 12) as a result of choosing the conjugate distribution parameters to best fit the tail. For full constellations with a long service history, the differences are much smaller (Table 9) and the prior distribution has little impact on the posterior distribution. In the case of low k value it may be more appropriately argued that the *no prior information* rule should be applied. Therefore, *Jeffrey's* prior is employed for the remainder of the paper.

6. FAULT HISTORY

Consider the fault history of the existing constellations, GPS and Glonass. A data mining approach presented in (Heng et. al., 2010; Heng, 2012) found a total of 28 *potential* GPS anomalies over the period 2004 to mid-2012. Here an anomaly is defined with respect to the service commitments, when the instantaneous user ranging error exceeds 4.42 times the URA (GPS, 2008). The anomalies are *potential* as they have not been fully verified in an independent manner and any faults lasting less than 15 minutes may not be included. Of the 28 potential anomalies, 21 were clock faults and fit the continuous definition.

Using the posterior distribution given by *Jeffrey's* prior:

$$\boldsymbol{f\left(\lambda|k,0,\tfrac{1}{2}\right) = \frac{e^{-\lambda}\lambda^{k-\frac{1}{2}}}{\Gamma\left(k+\frac{1}{2}\right)}} \tag{10}$$

and the fault history obtained by Heng *et. al.* (2012) gives the confidences for the true past mean failure probability shown in Table 4. Note that a constellation of 30 satellites is assumed for the purposes of transforming to a per satellite basis. This gives a total number of hourly periods of 2235330 over the 8½ year period.

Table 4. GPS Failure Rate Confidence

Percentile	P_{onset}/hr/sat All Faults	P_{onset}/hr/sat Cts Time Faults
95%	1.7×10^{-5}	1.4×10^{-5}
99%	1.9×10^{-5}	1.6×10^{-5}
99.9%	2.2×10^{-5}	1.8×10^{-5}
$1\text{-}10^{-5}$	2.6×10^{-5}	2.2×10^{-5}
$1\text{-}10^{-7}$	3.0×10^{-5}	2.5×10^{-5}
$1\text{-}10^{-9}$	3.3×10^{-5}	2.8×10^{-5}

Table 4 shows that whilst values greater than the service commitments are obtained for all confidence levels larger than 95%, the inflation of 10^{-5} is not excessive. The relationship between confidence percentile and failure rate is approximately log-linear. Confidence bounds up to 10^{-9} are presented as this presents the lower bound on risks which must be mitigated, known to have potentially *catastrophic* consequences in civil aviation (EASA, 2012). A confidence level is considered rather than fault rate but this provides some justification to the range of percentiles.

The highest confidence percentile of 10^{-9} requires a reasonable inflation factor of only 2.8 over the GPS service commitments. However, note that the discrete time faults addressed in section 8 must also be included.

Heng (2012) also analyses the Glonass fault history. Using an arbitrary fault threshold of the IURE of 50m (no public service commitments exist for Glonass) a total of 192 potential anomalies were identified between 2009 to August 2012. Using this result, Table 5 presents the equivalent confidence levels of the Glonass failure rate based on the assumption of a 24 satellite constellation. This gives a total number of hourly periods of 777888 over the assessment period in (Heng, 2012).

Table 5. Glonass Failure Rate Confidence

Percentile	P_{onset}/hr/sat All Faults
95%	2.8×10^{-4}
99%	3.0×10^{-4}
99.9%	3.1×10^{-4}
$1\text{-}10^{-5}$	3.4×10^{-4}
$1\text{-}10^{-7}$	3.6×10^{-4}
$1\text{-}10^{-9}$	3.8×10^{-4}

Using the data from (Heng, 2012), the Glonass failure rates are an order of magnitude greater than those of GPS. The log-linear relationship is preserved and a high confidence leads to only a reasonable inflation over the best estimate.

This section has presented the results of the methodology using the best available fault history data from (Heng, 2012), but the approach could be re-applied using different failure thresholds to obtain appropriate results. This is particularly relevant for Glonass in which reference (Heng, 2012) utilised a threshold of 50m, which is large with respect to some applications.

7. NEW CONSTELLATIONS

In section 6, the inference methodology was applied to fault history data of the existing constellations. In this section, the failure rates are derived for new constellations, such as Galileo or Beidou, or new blocks of satellites which may require a reset of the fault history.

Consider the failure rates with given confidences as a function of the observation window T, starting at an initial operating capability. It is assumed for the analysis that no faults are observed over this period but to maintain conservatism, a value of $k = 1$ is used, thereby extending the applicability of the derived values in the immediate period following a failure.

Table 6. Derived Failure Probabilities vs. Constellation Operational Time

Total Operational Time	P_{onset}/const
6 months	5.4×10^{-3}
1 year	2.7×10^{-3}
2 years	1.3×10^{-3}
5 years	9.1×10^{-4}
10 years	5.5×10^{-4}
20 years	2.7×10^{-4}
30 years	1.8×10^{-4}
50 years	5.5×10^{-5}
75 years	3.6×10^{-5}
100 years	2.7×10^{-5}

Table 6 shows the total (fault-free) operational time of a constellation of 24 satellites and the corresponding derived probability of failure with a confidence of $1\text{-}10^{-9}$.

8. DISCRETE TIME EVENTS

In the previous sections the NHPP was used to model the failure rate for punctual continuous time fault events. Consider discrete time failures which occur over a sample period such as incorrect ephemeris parameters. A temporal correlation exists between the presence of a fault at neighbouring times. This may be over the standard navigation message period of applicability (2 hours for GPS) or up to a maximum of the data period used for orbit determination (48 hours).

For discrete events, the appropriate model is an *inhomogenous* Binomial process, but no simplification to the standard Binomial process through taking the mean over time exists. Instead

the real process is considered to be a sequence of events with probability of failure $s = \{p_1, p_2, p_3 \ldots\}$ and the following assumption is imposed:

H3. The sequence s is non-increasing ($p_k \geq p_{k+1}$)

This is a stronger condition than hypotheses H1 and H2 applied in the continuous time case. It only applies to the navigation message type faults which depend on the ground network and may be understood as the ground network does not degrade over time. Under this assumption the standard Binomial process model is used to conservatively infer the posterior distribution for the current p based on past fault data.

$$\binom{n}{k} p^k (1-p)^{n-k} \tag{11}$$

where: $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

k the number of failure events

n the number of independent samples

p_i the true probability of fault during a single independent sample indexed by i

The conjugate prior distribution to the binomial is the beta distribution (Johnson and Kotz, 1995).

$$f(p) \sim p^{\alpha-1}(1-p)^{\beta-1} \tag{12}$$

The Jeffrey's prior parameter values to minimise the impact of prior information for the beta distribution are: $\alpha = \frac{1}{2}$ & $\beta = \frac{1}{2}$ which give the following posterior distribution.

$$f(p|k,n) \sim p^{k-1/2}(1-p)^{n-k-1/2} \tag{13}$$

The percentiles are determined by integrating up to the fault probability. Whilst the true time between independent navigation messages remains open to debate, values of 2 hours (nominal navigation message validity, 4 hours (nominal curve fit period), 12 hours (approximate orbital period) and 48 hours (data period used for orbit modelling) are used. These correlation times lead to numbers of samples of 898272, 449136, 149712 and 37428 on the basis of a 24 satellite constellation operating from the 1st Jan 2004 to 16th July 2012, being the period employed in (Heng, 2012). Table 7 shows the probability of failure per sample following the integration of the posterior distribution, whilst Table 8 converts these values to per hour figures.

Table 7. GPS Discrete Failure Rate Confidence

Percentile	P_{onset}/sample/sat Discrete Time Faults
	Independent sample period

	2hr	4hr	12hr	48hr
95%	1.4×10^{-5}	2.2×10^{-5}	8.3×10^{-5}	3.3×10^{-4}
99%	1.6×10^{-5}	3.4×10^{-5}	1.0×10^{-4}	4.1×10^{-4}
99.9%	1.8×10^{-5}	4.2×10^{-5}	1.3×10^{-4}	5.0×10^{-4}
$1\text{-}10^{-5}$	2.2×10^{-5}	5.6×10^{-5}	1.6×10^{-4}	6.7×10^{-4}
$1\text{-}10^{-7}$	2.5×10^{-5}	6.9×10^{-5}	2.1×10^{-4}	8.3×10^{-4}
$1\text{-}10^{-9}$	2.8×10^{-5}	8.2×10^{-5}	2.5×10^{-4}	9.8×10^{-4}

Table 8. GPS Discrete Failure Rate Confidence per hour

Percentile	P_{onset}/hr/sat Discrete Time Faults			
	Independent sample period			
	2hr	4hr	12hr	48hr
95%	5.7×10^{-6}	5.7×10^{-6}	7.0×10^{-5}	7.0×10^{-6}
99%	8.5×10^{-6}	8.5×10^{-6}	8.5×10^{-6}	8.5×10^{-6}
99.9%	1.0×10^{-5}	1.0×10^{-5}	1.0×10^{-5}	1.0×10^{-5}
$1\text{-}10^{-5}$	1.1×10^{-5}	1.4×10^{-5}	1.4×10^{-5}	1.4×10^{-5}
$1\text{-}10^{-7}$	1.7×10^{-5}	1.7×10^{-5}	1.7×10^{-5}	1.7×10^{-5}
$1\text{-}10^{-9}$	1.7×10^{-5}	2.0×10^{-5}	2.0×10^{-5}	2.0×10^{-5}

and show higher confidence is obtained without an extreme increase in the failure rate reflecting the continuous case. Although the larger correlation time decreases the number of samples, due to the factoring by the period, Table 8 shows only a minor sensitivity to this assumption. Note however, that the longer correlation time faults could be subject to longer exposure times if there are no guarantees of detection by the control segment. Alternatively, a more complex model could be employed to reflect this (Blanch, 2012).

Considering the discrete model for new systems or constellations gives confidence levels on the probability of failure as shown in Table 9.

Table 9. Derived Failure Probabilities vs. Constellation Operational Time

Total Operational Time	Independent sample period
6 months	4.5×10^{-3}
1 year	2.4×10^{-3}
2 years	1.2×10^{-3}
5 years	5.0×10^{-4}
10 years	2.5×10^{-4}
20 years	1.3×10^{-4}
30 years	8.5×10^{-5}
50 years	5.1×10^{-5}
75 years	3.4×10^{-5}
100 years	2.6×10^{-5}

9. ALL EVENTS MODEL

In order to summarise the steps required to arrive at the bounds of the total failure rate as given in Table 10, Figure 6 presents the process in full.

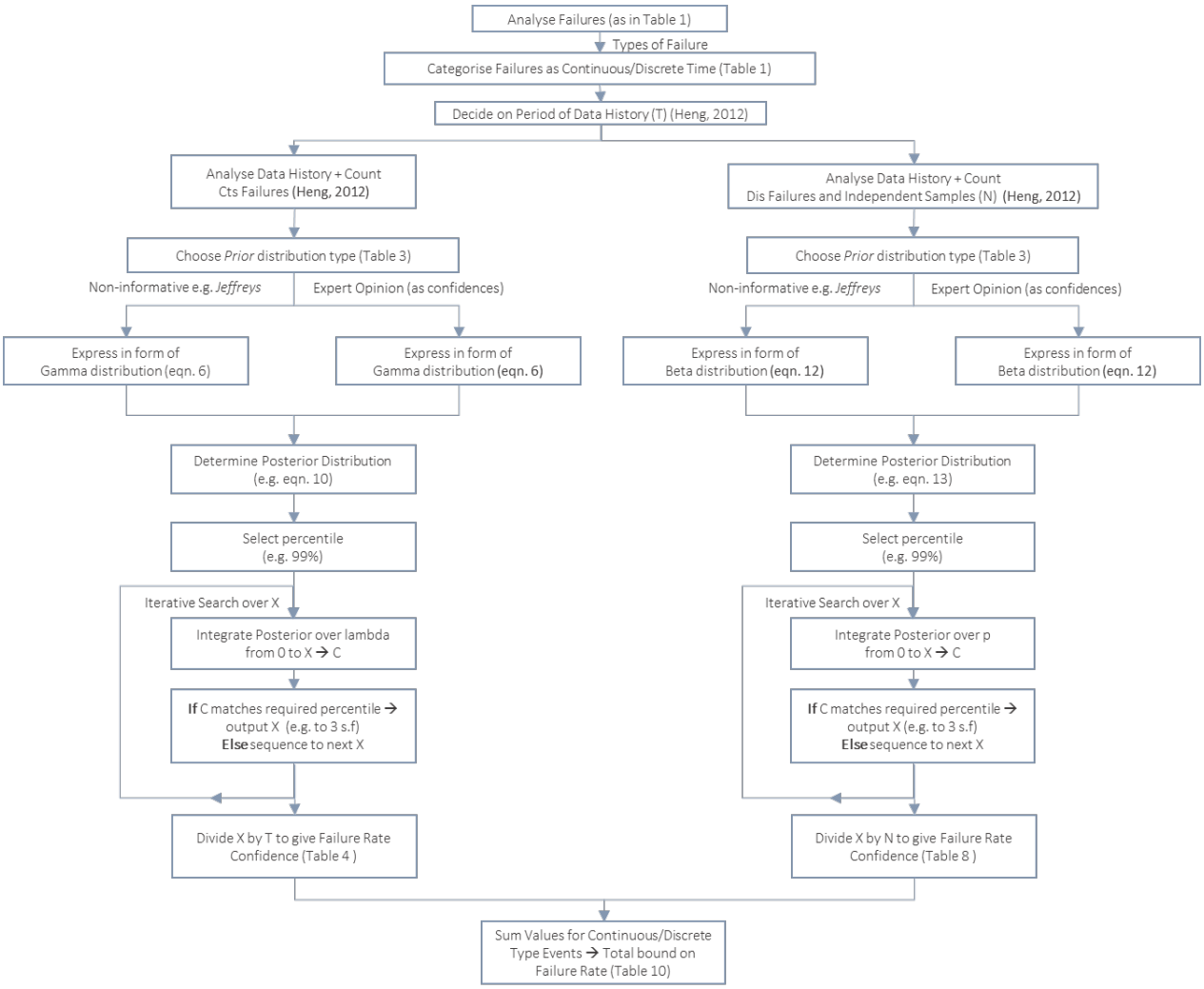

Figure 6: Failure Rate Bounding Process

The results provided in sections 6 and 8 to complete a table of the total probability of failure per hour and per satellite using the more conservative 48 hour sample period.

Table 10. GPS Total Failure Rate Confidence

	P_{onset}/hr/sat		
Percentile	Continuous	Discrete	Total
95%	1.4×10^{-5}	7.0×10^{-6}	2.1×10^{-5}
99%	1.6×10^{-5}	8.5×10^{-6}	2.4×10^{-5}
99.9%	1.8×10^{-5}	1.0×10^{-5}	2.8×10^{-5}

$1\text{-}10^{-5}$	2.2×10^{-5}	1.4×10^{-5}	3.6×10^{-5}
$1\text{-}10^{-7}$	2.5×10^{-5}	1.7×10^{-5}	4.2×10^{-5}
$1\text{-}10^{-9}$	2.8×10^{-5}	2.0×10^{-5}	4.8×10^{-5}

Table 10 shows that in order to have a high confidence, factors of the order of 2 to 5 are required based on the fault history provided in (Heng, 2012). Table 11 presents the equivalent total failure model for the case of new satellite constellations or blocks and the associated operational time.

Table 11. Operational Time

	P_{onset}/const			P_{onset}/sat (24)
Total Operational Time	Cts	Dsc	Total	Total
6 months	5.4×10^{-3}	4.5×10^{-3}	1.0×10^{-2}	4.2×10^{-4}
1 year	2.7×10^{-3}	2.4×10^{-3}	5.1×10^{-3}	2.1×10^{-4}
2 years	1.3×10^{-3}	1.2×10^{-3}	2.5×10^{-3}	1.0×10^{-4}
5 years	9.1×10^{-4}	5.0×10^{-4}	1.4×10^{-3}	5.8×10^{-5}
10 years	5.5×10^{-4}	2.5×10^{-4}	8.1×10^{-4}	3.3×10^{-5}
20 years	2.7×10^{-4}	1.3×10^{-4}	4.0×10^{-4}	1.7×10^{-5}
30 years	1.8×10^{-4}	8.5×10^{-5}	2.7×10^{-4}	1.1×10^{-5}
50 years	5.5×10^{-5}	5.1×10^{-5}	1.0×10^{-4}	4.2×10^{-6}
75 years	3.6×10^{-5}	3.4×10^{-5}	7.0×10^{-5}	2.9×10^{-6}
100 years	2.7×10^{-5}	2.6×10^{-5}	5.3×10^{-5}	2.2×10^{-6}

10. CONCLUSIONS

This work has presented a novel approach to the setting of failure probability assumptions for GNSS safety, liability and mission critical applications. A methodology has been defined whilst carefully stating the assumptions needed to infer future reliability statistics based on past data. Results have been presented for two intrinsic fault types, continuous faults which are punctual events occurring at any continuous point in time and discrete faults whose occurrence is tied to an independent single sample. This dichotomy is crucial so not to model certain fault types using an inappropriate model.

Confidence bounds have been determined for the failure probability of continuous faults in the range of 1-3 times larger than the service commitment of 10^{-5} per hour per satellite with extremely high confidence. This suggests that the analysis matches well the service commitments but could enable a quantified layer of conservatism to be applied. Similarly, for the discrete time events, conservative factors of 1-2 are determined. Therefore, for the total fault probability factors up to 5 are obtained. Application of the methodology to new blocks of satellites has shown how quickly confidence could be gained from a new constellation or modernization programs in the absence of failures.

The natural objection to this analysis is whether applying inferences on past data is applicable to future failure probability predictions. However, such inductive argument is intrinsic to the service commitment statements and any other statements relating to future performance.

The step forward taken by this paper is in introducing a quantifiable conservative bound avoiding the need for arbitrary assumptions. The probability of failure is considered a random time varying parameter whose distribution is estimated rather than deriving a more simplistic point estimate. Secondly, justification is given to using inference on past data for future operations. From the point of view of a fastidious system designer, this paper gives confidence to the existing GPS performance commitments with some small conservative factors applied to provide the confidence margins preferred. The paper also shows the approach applied to new constellations with limited fault histories (e.g. Galileo). In future, informative priors could be included to take account of an FMEA undertaken within the constellation design, testing and validation.

APPENDIX

This appendix presents tables giving the confidence bounds for different failure number cases and for each of the priors considered in the paper.

ID	Expert	10^{-3}	10^{-5}	10^{-7}	10^{-9}
1	Uniform	9.23	14.24	19.12	23.94
2	Albert	6.91	11.51	16.12	20.72
3	Jeffrey	8.13	12.95	17.70	22.42
4	Positive	11.87	16.97	21.81	26.50
5	Realistic	12.44	17.78	22.84	27.77
6	Conservative	11.92	17.28	22.40	27.39
7	Highly	11.17	16.47	21.56	26.54

Table 12: $\boldsymbol{k = 1}$ confidence bounds

ID	Expert	10^{-3}	10^{-5}	10^{-7}	10^{-9}
1	Uniform	11.23	16.55	21.67	26.67
2	Albert	9.23	14.24	19.12	23.94
3	Jeffrey	10.26	15.43	20.43	25.35
4	Positive	13.45	18.77	23.78	28.61
5	Realistic	14.09	19.66	24.91	29.97
6	Conservative	13.67	19.28	24.60	29.74
7	Highly	12.99	18.57	23.87	29.01

Table 13: $\boldsymbol{k = 2}$ confidence bounds

ID	Expert	10^{-3}	10^{-5}	10^{-7}	10^{-9}
1	Uniform	24.13	31.17	37.57	43.63
2	Albert	22.66	29.52	35.79	41.74
3	Jeffrey	23.40	30.35	36.69	42.69
4	Positive	24.57	31.26	37.31	43.00
5	Realistic	25.74	32.75	39.08	45.04
6	Conservative	25.79	32.93	39.39	45.48
7	Highly	25.46	32.63	39.13	45.25

Table 14: $\boldsymbol{k = 10}$ confidence bounds

ID	Expert	10^{-3}	10^{-5}	10^{-7}	10^{-9}
1	Uniform	51.08	60.67	69.06	76.77
2	Albert	49.80	59.29	67.60	75.24
3	Jeffrey	50.44	59.98	68.33	76.01
4	Positive	48.75	57.66	65.43	72.56
5	Realistic	51.08	60.40	68.54	76.01
6	Conservative	51.95	61.51	69.85	77.51
7	Highly	52.10	61.74	70.17	77.91

Table 15: $\boldsymbol{k = 3}$ confidence bounds

DISCLAIMER

The views and conclusions expressed in this paper are those of the authors only and do not reflect official standpoints of any organization or working group.

REFERENCES

Global Positioning System (2008) Standard Positioning Service Performance Standard, 4th Edition, September 2008. Department of Defense/Department of Transportation

Global Positioning System (2001) Standard Positioning Service Performance Standard, 3rd Edition, October 2001. Department of Defense/Department of Transportation

Van Dyke, K., Kovach, K., Kraemer, J., Lavrakas, J., Fernow, J.P., Reese, J., Attallah, N., Baevitz, B., (2003). GPS Integrity Failure Modes and Effects Analysis. *Proceedings of the 2003 National Technical Meeting of The Institute of Navigation, Anaheim, CA, January 2003, pp. 689-703.*

Van Dyke, K., Kovach, K., Lavrakas, J., Carroll, B. (2004) Status Update on GPS Integrity Failure Modes and Effects Analysis. *Proceedings of the 2004 National Technical Meeting of The Institute of Navigation, San Diego, CA, January 2004, pp. 92-102.*

ICAO (2010) Annex 10, Aeronautical Telecommunications, Volume 1 (Radio Navigation Aids), Amendment 86, effective 17 November 2011. GNSS standards and recommended practices (SARPs) are contained in Section 3.7 and subsections, Appendix B, and Attachment D.

Pullen, S., Rife, J., Enge, P. (2006) Prior Probability Model Development to Support System Safety Verification in the Presence of Anomalies. *Proceedings of IEEE/ION PLANS 2006, San Diego, CA, April 2006, pp. 1127-1136.*

Lee, Y. C., Van Dyke, K. L. (2002) Analysis Performed in Support of the Ad-Hoc Working Group of RTCA SC-159 on RAIM/FDE Issues. *Proceedings of the 2002 National Technical Meeting of The Institute of Navigation, San Diego, CA, January 2002, pp. 639-654.*

RTCA (2004) WAAS Minimum Operational Performance Specification (MOPS), RTCA document DO-229D

FAA (2010) Phase II of the GNSS Evolutionary Architecture Study, February 2010

Blanch, J., Walter, T., Enge, P., Wallner, S., Amarillo-Fernandez, F., Dellago, R., Ioannides, R., Hernandez-Fernandez, I., Belabbas, B., Spletter, A., Rippl, M. (2013) Critical Elements for a Multi-Constellation Advanced RAIM. *NAVIGATION, Journal of The Institute of Navigation, Vol. 60, No. 1, Spring 2013, pp. 53-69.*

WG-C (2012) Milestone I Report Working Group C ARAIM Technical Subgroup, EU-US Cooperation of Satellite Navigation

Murphy, T., Harris, M., Pullen, S., Pervan, B., Saito, S., Brenner, M. (2010) Validation of Ionospheric Anomaly Mitigation for GAST D. *Working paper presented at Working group of the whole meeting, ICAO NSP May 2010 WGW/WP14*

Blanch, J. (2010) Briefing at the EU-US Working Group C ARAIM Subgroup, April 2012

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

Shively, C. (1999) Analysis of Probability of Misleading Information for LAAS Signal In Space. *Proceedings of ION National Technical Meeting, San Diego, CA, 25 – 27 January 1999.*

DeCleene, B. (2000) Defining Pseudorange Integrity – Overbounding. *Proceedings of the 13th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 2000), Salt Lake City, UT, September 2000, pp. 1916-1924.*

Lee, J., Pullen, S. and Enge, P. (2006) ". *IEEE Trans. Aerospace and Electronic Systems Vol. 42, No. 2 APRIL 2006*

Sturza, M. (1989) Navigation System Integrity Monitoring Using Redundant Measurements. *NAVIGATION, Journal of The Institute of Navigation, Vol. 35, No. 4, Winter 1988-1989, pp. 483-502.*

van Graas, F. and Zhu, Z. (2011) Tropospheric Delay Threats for the Ground Based Augmentation System. *Proceedings of the 2011 International Technical Meeting of The Institute of Navigation, San Diego, CA, January 2011, pp. 959-964.*

O'Hagan, A. and Forster, J. (2003) Kendall's Advanced Theory of Statistics, Volume 2B: Bayesian Inference. *Arnold, New York. ISBN 0-340-52922-9.*

Neyman, J. (1937) Outline of a Theory of Statistical Estimation Based on the Classical Theory of Probability. *Philosophical Transactions of the Royal Society of London A, 236, 333–380.*

Fraser, D.A.S (2011) Is Bayes Posterior just quick and dirty confidence? *Statistical Science*, vol. 26, pp. 299-316

Cox, D. R. and Isham, V. I. (1980). Point Processes. *Chapman & Hall. ISBN 0-412-21910-7.*

Pham, Hoang (2006) Software Reliability Modeling. *System Software Reliability. Springer Series in Reliability Engineering. pp. 153–177*

Raiffa, H and Schlaifer R.(1961) Applied Statistical Decision Theory. Division of Research, Graduate School of Business Administration, Harvard University, 1961

Box, G. E. P. and Tiao, G. C. (1973) Bayesian Inference in Statistical Analysis. *Wiley, ISBN 0-471-57428-7*

Jeffreys, H. (1946) An Invariant Form for the Prior Probability in Estimation Problems. *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences 186 (1007): 453–461*

Heng, L. (2012) Safe Satellite Navigation with Multiple Constellations: Global Monitoring of GPS and GLONASS Signal-In-Space Anomalies. *Ph.D. Dissertation, Stanford University, December 2012*

EASA (2012) Certification Specifications and Acceptable Means of Compliance for Large Aircraft, CS-25, EASA, July 2012

Johnson, N. L., Kotz, S., Balakrishnan, N. (1995) Continuous Univariate Distributions Vol. 2. *Wiley*