



DYNAMIC POSITIONING CONFERENCE
October 12-13, 2010

SENSOR I

High Integrity Positioning:

Lessons from the Aviation Industry

**Mark Ahlbrecht, Gary Wolanin, Kevin Vanderwerf, Jim McDonald,
Mike Ibis, Curt Call**

**Honeywell Aerospace
(Coon Rapids, MN, USA)**

Abstract

The International Marine Organization's (IMO) e-Navigation concept of an integrated onboard navigation system defines as a core element "high integrity electronic positioning". This positioning capability would demonstrate defined levels of accuracy, integrity and continuity appropriate to a safety critical system.

High integrity positioning presents challenging issues to an integrated navigation system:

- Different operations require different levels of integrity.
- Integrity of the navigation solution can be difficult to quantify, especially in integrated systems.
- Integrity of the navigation solution may change over time.
- Navigation systems need to protect the integrity of the end solution from corruption in the presence of a failure.

The aviation industry has been using high integrity positioning and performing complex, safety critical operations for many years. Examination of the methods of handling high integrity positioning and operations in aviation could illuminate solutions for the marine industry. This paper will share the methods and tactics from the aviation industry used to produce high integrity positioning and perform safety critical operations. The trade-off involved with navigation system accuracy, integrity, continuity and availability are discussed. Similarities, and potential synergies, between aviation navigation design and marine navigation are identified.

Navigation System Requirements

There are four main requirements applied to navigation systems in a general sense. These requirements are accuracy, integrity, continuity and availability.

Accuracy is the degree of conformance between the measured position and the true position of the vessel. Accuracy requirements are typically driven by the needs of the system to provide performance from one operation to another. Positioning accuracy requirements are expressed in a positioning sense (meters, nautical miles, etc.).

Integrity is the ability to provide timely warnings to users when the system should not be used for navigation. Any system with integrity needs to provide an estimate of the quality of the navigation output. If this quality is a conservative representation of the actual error then all that is required to perform a given operation is to compare this quality value to the maximum allowable error limit. This maximum allowable error is termed the alarm limit. This alarm limit can be a function of the operation. If the actual error is greater than the indicated quality then the sensor is providing misleading information. If the system is providing misleading information and the actual error is greater than the alarm limit then the system is providing hazardously misleading information (HMI). These conceptual states are illustrated in Figure 1. The risk to the navigation user is that the navigation system is providing HMI for an unacceptably long period of time. The acceptable period of time is known as the time to alarm (TTA). Integrity requirements are framed as the allowable probability of hazardously misleading information for greater than the time to alarm.

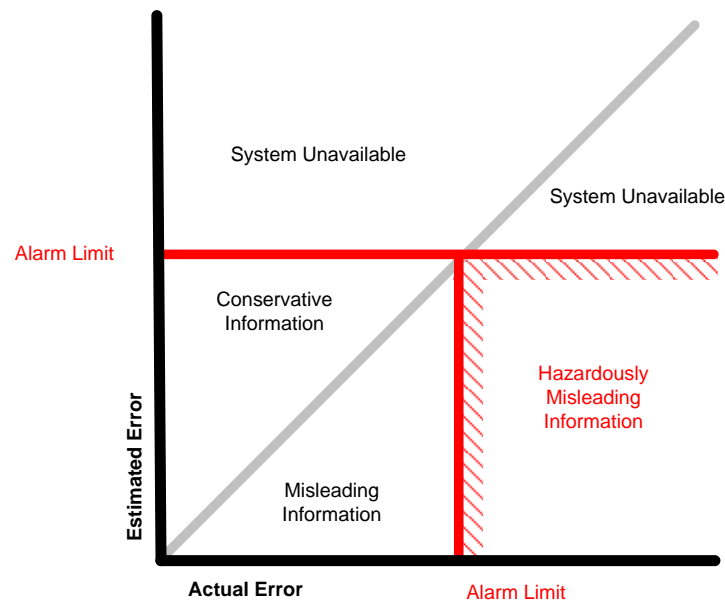


Figure 1

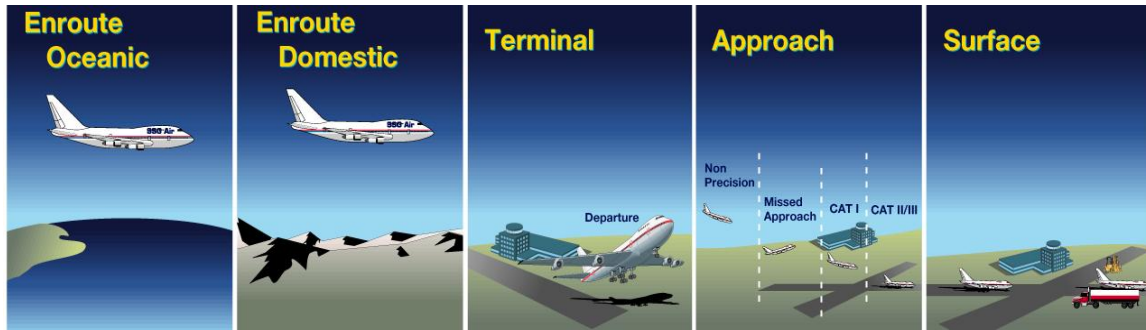
Continuity is the probability that the system will operate within defined performance limits for an intended period of operation. More specifically continuity is the probability that the specified system performance will be maintained for the duration of the phase of the operation, presuming the system was available at the beginning of that operation and predicted to operate throughout the operation. [3]

Availability is the percentage of time the system satisfies all the accuracy, integrity and continuity requirements at the initiation of the intended operation [3]. Availability is a measure of how usable the system is when the other safety requirements are met.

In the design of navigation systems there is a tradeoff between these four requirements. If all other things are held constant and the accuracy improves, then the integrity as well as continuity and availability will improve. If the integrity improves (i.e. is safer) and the accuracy stays the same, then the continuity and availability will be reduced. If the continuity/availability is increased and the accuracy stays the same then integrity will be reduced (i.e. less safe).

Navigation System Requirements in Aviation

Phases of flight in aviation have different risk factors for safety. For example, an aircraft on an ocean crossing only has to be concerned with navigating to the general vicinity of their destination as well as avoiding sparse traffic. As a result, the oceanic safety requirements are fairly loose. In a Category III precision landing which includes flaring the aircraft and guiding it down the runway, small navigation errors create a high risk of hazardous operation; therefore the accuracy and integrity requirements are very stringent. Once a precision approach is started it greatly increases the pilot workload if it becomes necessary to abort due to a navigation system failure, so the continuity requirements are also stringent. Figure 2 shows the spectrum of navigation system requirements from oceanic to precision approach.



Performance Requirement	Oceanic	Domestic	Terminal	Approach	Cat III Landing
Risk Factor	Traffic	Traffic	Traffic/Terrain	Terrain	Terrain
Accuracy Horz/Vert	10 nm	2 nm	220 m	220m – 16m	6.2 m / 2.9-6.7 ft
Integrity – P(HMI)	10^{-7} / hr	10^{-7} / hr	10^{-7} / hr	2×10^{-7} / approach	10^{-9} / approach
Horizontal Alert Limit	20 nm	4 nm	1 nm	0.3 nm – 40m	15.5 m/4.4m
Time To Alert	300 sec	15 sec	15 sec	10 – 6 sec	3.0 sec
Continuity	10^{-8} /hr	10^{-8} /hr	10^{-8} /hr	1.8×10^{-6} / 15 sec	1.8×10^{-6} / 15 sec
Availability	0.99 – 0.99999%	0.99 – 0.99999%	0.99 – 0.99999%	0.99 – 0.99999%	0.99 – 0.99999%

Figure 2

Historically operations were based on a specific navigation system. These could be VOR, DME, GPS, or ILS. Airborne equipment for these operations was certified to a common minimum operating standard developed by industry (See [3]) and instantiated by regulatory authorities. Recently however, there has been a shift to developing system level requirements for the approach and allowing various solutions to be developed to meet those requirements. This more modern type of operation is termed Required Navigation Performance (RNP) Operations

The Required Navigation Performance concept allows aircraft to operate in a defined airspace based on the available navigation performance of its equipment. The navigation performance is defined in terms of the accuracy, integrity, availability and continuity of the system.

“Navigation performance” for RNP operations is decomposed into three error components. The Navigation System Error (NSE) is the error from the true position to the estimated position. This error is a function of the navigation system and sensor quality. The Flight Technical Error (FTE) is the difference between the position determined by the navigation system and the defined

position. FTE is a function of the control system on the vehicle. There is also a Path Definition Error (PDE) component between the position defined in the operation and the desired position. This error is a survey or operation design error. Figure 3 illustrates these components. Total System Error (TSE) is the sum of NSE and FTE and represents the total error from the defined path. RNP operations are defined in terms of TSE, so NSE and FTE can be traded off.

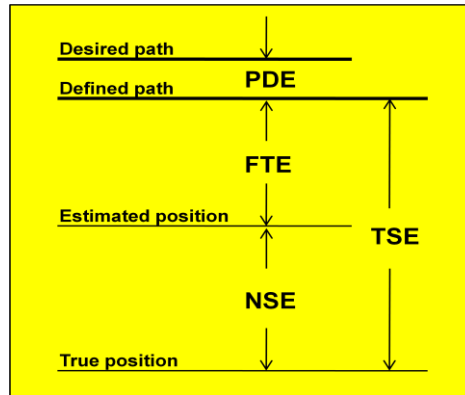


Figure 3

Aircraft equipment that is part of an integrated navigation system providing positioning data to support RNP operations transmits parameters that statistically bound the position error. These outputs include a Horizontal Figure of Merit (HFOM), a Horizontal Integrity Level (HIL) and a detection alert as a minimum.

The HFOM is the 95% estimate of the position errors in the horizontal plane assuming no GPS satellite integrity failures and is used to quantify accuracy.

The HIL provides the horizontal region of protection at the required integrity given an undetected failure is present. The HIL is based on the error models using satellite geometries and vehicle trajectory data and is not influenced by the input measurement data.

A detection alert occurs once when the system estimates that there is a failing satellite is present. A missed alert is defined when the actual position error exceeds the HIL for more than the time to alert. A missed alert negatively effects integrity. A false alert is defined as a detection alert that is issued when no failure condition exists. A false alert negatively effects continuity. Once the error has been detected, the system attempts to isolate the failure and then exclude it from the solution. Continuity is increased when a system can detect and exclude satellite errors before they interfere with an intended operation.

Guidance equipment can use these signals to decide if the navigation system error supports a given phase of flight or RNP performance level. For example, the HIL can be compared to a specific Horizontal Alert Limit (HAL) defined as a containment level for that operational procedure. Therefore, improved performance that lowers the HIL will provide additional availability for that HAL level. The relationship between RNP value and HAL depends on the unique performance characteristics for each airplane model, since it must account for flight technical error (FTE).

System Architectures for High Integrity Positioning

There are three common navigation system architectures for high integrity applications used to address the high integrity positioning trade-offs. These architectures are: a high reliability sensor, redundant architecture and an integrated architecture. These architectures are illustrated in Figure 4.

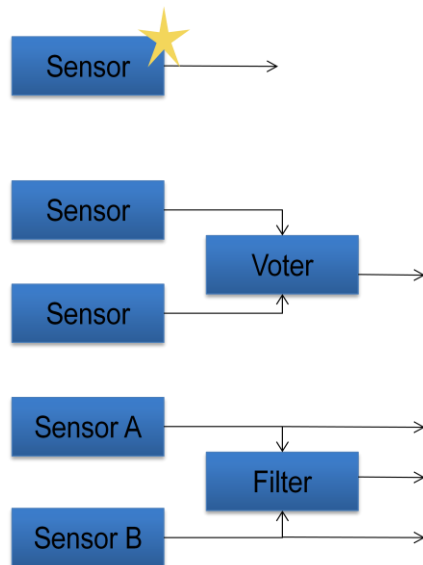


Figure 4

A high reliability sensor could be utilized. This higher reliability sensor would reduce the probability of failure leading to a higher integrity for a given accuracy. This architecture can get more costly as requirements get more stringent. This particular architecture may not be an option if the system is dependent on external systems (like GNSS).

A redundant architecture can add cost for the duplicate functionality. There can be an advantage in increasing continuity and availability after a failure. The disadvantage is that the voting system can add new failure modes and can create other independence issues.

An integrated architecture can take advantage of the safety benefits of different sensor classes and combine them, producing a high integrity position with properties better than either sensor class. One advantage is the availability of the integrity after a sensor class failure, say loss of GPS signal in space. Integrated architectures have a more complex physical architecture and analysis to assure integrity limits are properly determined for the different sensor classes. In aviation there has been a general trend to integrated architecture to harness the benefits of reduced cost, reduced weight and increased flexibility.

A High Integrity GNSS/IRS Integrated Architecture

Inertial Reference Systems (IRS) and Global Navigation Satellite System (GNSS) sensors are commonly integrated to achieve enhanced position accuracy and bandwidth. IRS and GPS can also be integrated to provide enhanced integrity, continuity and availability.

On an aircraft there are typically 2-3 inertial reference systems that provide heading, attitude, position, velocity and other parameters to the Flight Management Unit and displays. There are also typically 2 GNSS sensors that provide position and velocity information.

From a positioning standpoint, the IRS produces a position with a fixed integrity but an accuracy that grows over time. The GNSS sensor produces a position that has a time varying integrity due to the changes in the satellite geometry. By providing the IRS with the raw measurement data from the GPS receivers the IRS is able to combine that information with its measurement of motion to produce an improved integrity over the GNSS “snapshot” solution.

Figure 5 shows the interfaces between devices. The interfaces required for the integration are shown in red.

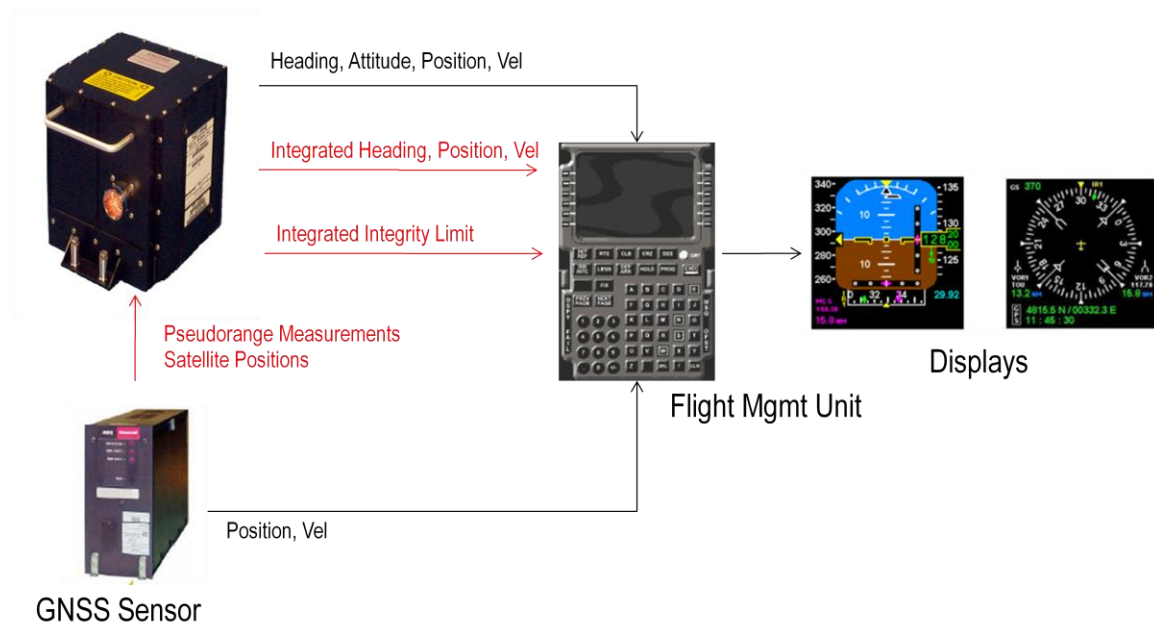


Figure 5

Integration Method

Kalman filters have been used for many years to blend sensors with complementary properties. This fusion has typically been driven by the need for increased accuracy, but can also be used to provide improved integrity, continuity, and availability.

An inertial system is very accurate over the short term but has errors that grow significantly over time. GPS, on the other hand, has relatively large short-term errors but good long-term bounded accuracy. GPS accuracy is dependent on satellite geometries which can be affected by signal masking and interference. One can easily see the possible advantages of blending these complementary systems with respect to accuracy performance. Honeywell’s INS/GPS Hybrid (HIGH) implementation uses a blending of GPS pseudo-range and pressure altitude measurements with inertial data using Kalman filtering techniques to provide an enhanced navigation performance which is better than possible with autonomous GPS systems.

While there are significant accuracy benefits with a hybrid system, providing valid satellite fault detection and exclusion (FDE) capability has proven to be a significant challenge. GPS is vulnerable to errors in the satellite signal in space. Typically autonomous GPS receivers use a “snapshot” Receiver Autonomous Integrity Monitor (RAIM) algorithm which is based only on information taken at a particular time so it is not influenced by previous measurements. Unfortunately the RAIM calculation requires redundant satellites and is only valid for that particular time. The inertial system is self contained so its performance is not vulnerable to external interference and common mode failures. Most commercial aircraft have redundant inertial systems to provide inertial integrity.

The inherent nature of a Kalman filter is that it retains a “memory” of previous measurements and error estimates in the current solution. Satellite failures that grow slowly may influence the solution before they can be detected. Even after the errant satellite has been excluded from the solution, the hybrid position will continue to be affected by the error for several minutes.

The solution separation method utilized in Honeywell’s HIGH implementation is one method which solves the issue of possible corrupted Kalman filter solutions. The (HIGH) solution utilizes multiple Kalman filters operating on various subsets of satellite measurements to form a blended integrity metric. The basic architecture of this integration method is shown in Figure 6.

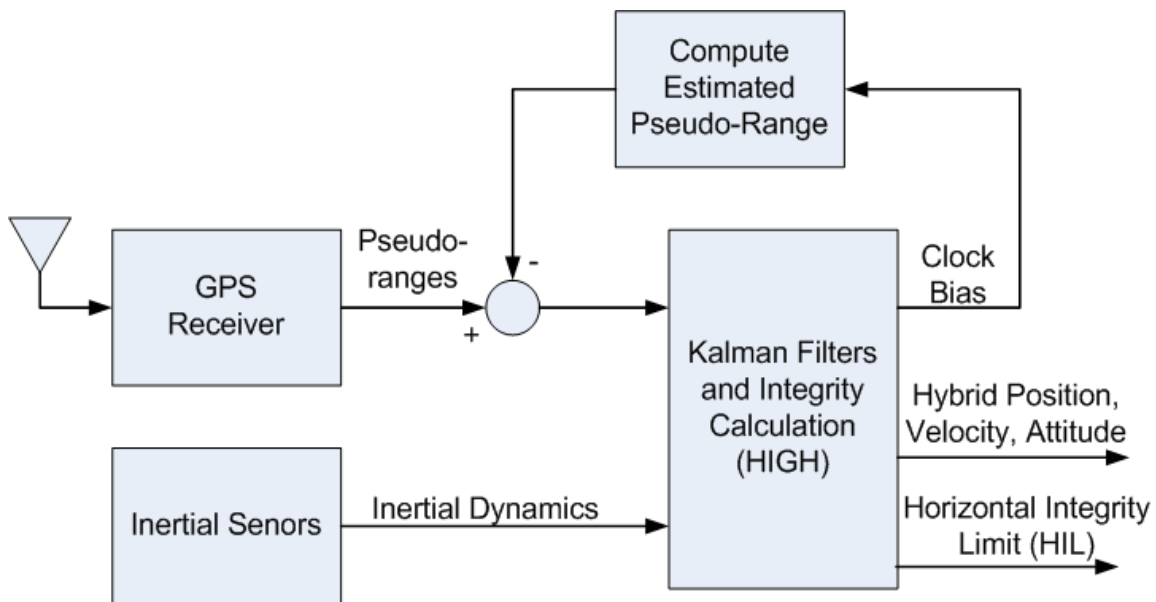


Figure 6

The solution separation method consists of multiple inertial/GPS hybrid position solutions using multiple Kalman filters. The complete set of filters includes a main filter, sub-filters, and sub-sub-filters. The main filter incorporates measurements from all N satellites in view. Each sub-filter of a set of N sub-filters incorporates measurements from a different combination of N-1 satellites. Fault detection occurs when the separation between the main filter’s solution and at least one of the sub-filter solutions exceeds a threshold that is based on the expected statistical separation and the allowable false alert rate. For each sub-filter, a set of N-1 sub-sub-filters exist each of which incorporates measurements only from the remaining N-2 satellites. The hierarchy of Kalman filter

solutions is shown in Fig. 7. The numbers indicate which satellites are excluded from that filter's solution.

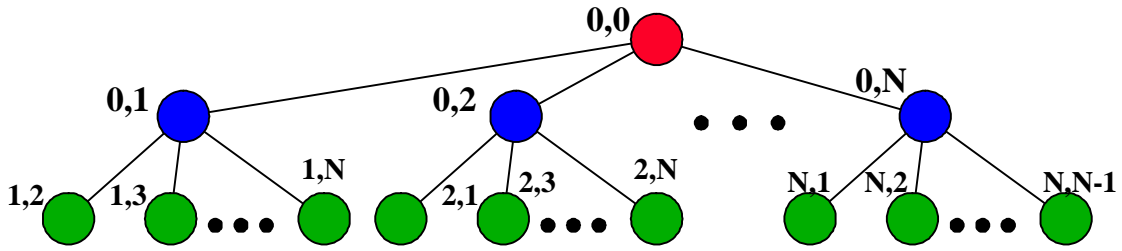


Figure 7

Once detection occurs, isolation and exclusion of the failed satellite is accomplished by examining the separation of each sub-filter position solution from each of its sub-subfilter solutions. If one and only one sub-filter is separated from each of its sub-sub-filters by less than the corresponding threshold, then that sub-filter is excluding the failed satellite in its solution.

Fig. 8 shows a high-level block diagram of the HIGH implementation of solution separation. The error states from the main filter are used to correct the inertial navigation solution which provides the hybrid solution (position, velocity, etc).

The sub-filter horizontal position solution separations from the main solution (dx_{0n}^{hpos}) are used to detect a failure by comparing the magnitude of each to its respective threshold (D_{0n}). The threshold is determined by scaling the one-sigma separation (σ_{d0n}) in the worst-case direction as determined from the corresponding separation covariance matrix (dP_{0n}^{hpos}). The scaling multiplier K_{fd} is chosen to achieve the allowable false alarm rate of $10^{-5}/hr$. In addition, an HIL corresponding to each sub-filter is computed by adding a value to the threshold that bounds sub-filter position error to a probability $1-p_{md}$ (where p_{md} is the allowed missed detection probability of 0.001). The resulting sum bounds the main filter's position to the same probability given the worst case undetected failure in that satellite.

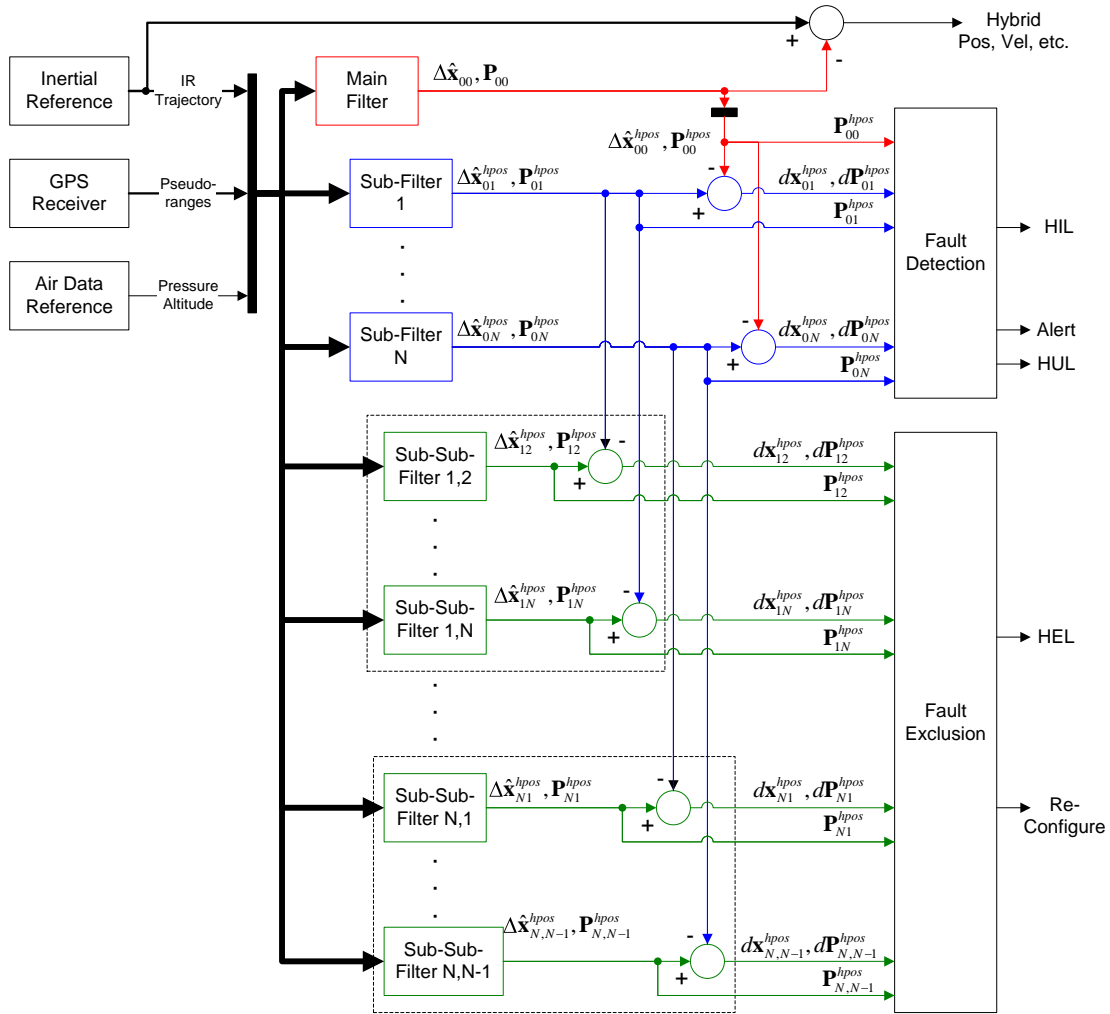


Figure 8

Fig. 9 illustrates the HIL calculation for one sub-filter (n) HIL for the faulted satellite hypothesis (H1). Fig. 10 further illustrates this HIL calculation in terms of the probability density function (PDF).

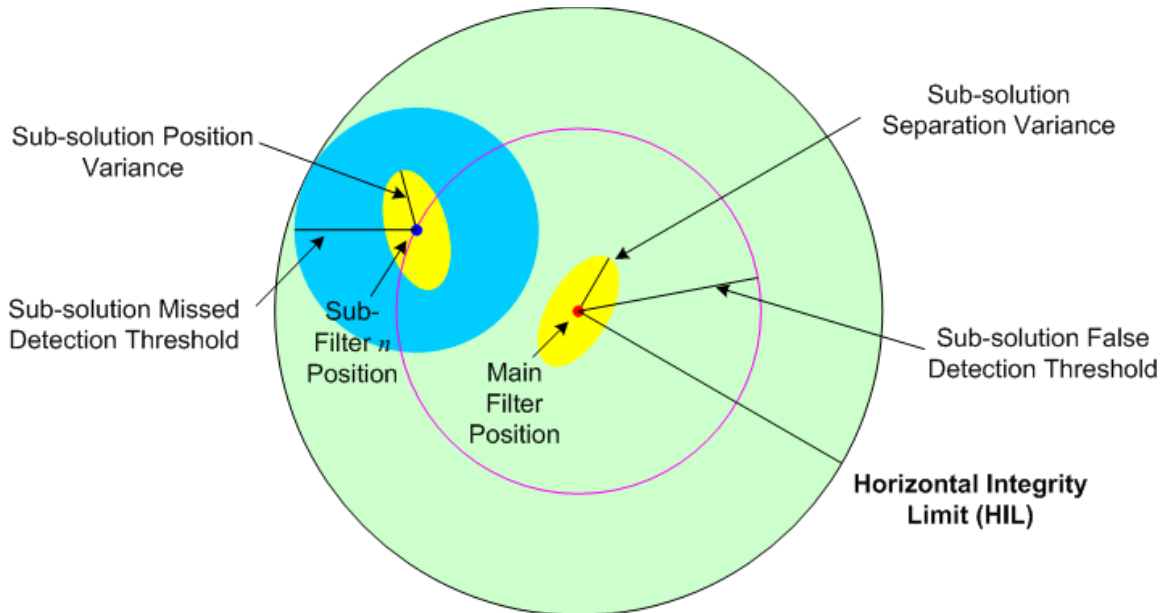


Figure 9

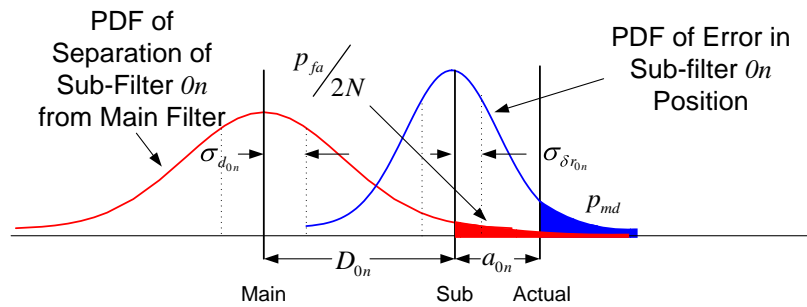


Figure 10

We must also consider the rare-normal fault-free hypothesis (H0). The fault-free HIL must bound the main filter position in the absence of satellite failures to the required integrity level. This is done by scaling the one-sigma position error of the main filter in the worst case direction ($\sigma_{\delta r_{00}}$) as determined from the main filter covariance matrix (P_{00}^{hpos}) as follows:

$$HIL_{ff} = K_{ff} \sigma_{\delta r_{00}}$$

The multiplier K_{ff} is chosen based on the error distribution to yield the required integrity level. Because the fault-free HIL is driven by inertial sensor performance and each inertial system is independent, the rare-normal integrity requirement is relaxed to $10^{-5}/hr$ (compared to the integrity requirement of $10^{-7}/hr$ for the H1 hypothesis). The overall HIL is the maximum of all of these HILs as follows:

$$HIL = \max(\max(D_{0n} + a_{0n}), HIL_{ff}), n=1, N$$

Isolation of the failed satellite is accomplished by performing detection on the separations between each sub-filter and its corresponding sub-sub-filters. Successful isolation occurs when each sub-filter has a detection alert except for the one sub-filter which excludes the failed

satellite. Upon successful isolation, the filters are all re-initialized using the one sub-filter that was not corrupted by the failure.

A more detailed explanation of Honeywell’s solution separation method has been documented in previous papers [1][2].

User Interface

Since different operations require different levels of integrity, the operator needs to know if the integrity being provided by the navigation system (HIL) meets the requirements of the intended operation (HAL). Figure 11 shows how the integrity information necessary for an operation is displayed on the aircrafts Primary Flight Display (PFD).

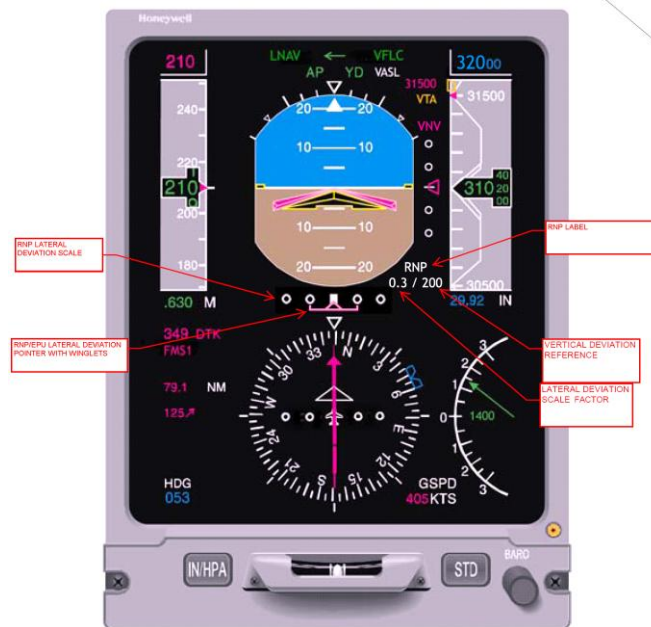


Figure 11

What is really important to the operator is the relativity of the two values (HIL and HAL). Figure 12 shows the detail of the PFD display when the integrity is sufficient and insufficient. Note that the offset in this display is the current Flight Technical Error (FTE).

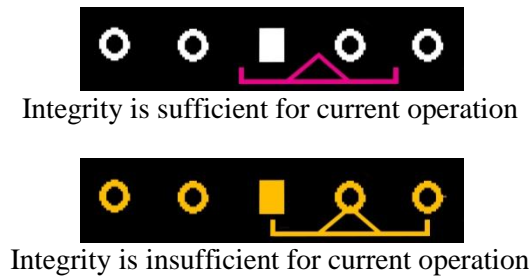


Figure 12

Benefits of Integration

Accuracy is improved by incorporation of inertial measurements with GPS measurements in an optimal manner. Although the positioning accuracy is dominated by the GPS performance in the long term, the additional information provided by the inertial sensors provides improved accuracy with in turn supports improved integrity, continuity, and availability.

Integrity is improved by the incorporation of the additional independent inertial sensors. The Kalman filter's ability to predict states allows the system to estimate position uncertainty and therefore HIL even when satellite measurements are not present; often referred to as "integrity coasting". This capability also means that a tightly coupled system is less reactive to geometry changes due to setting satellites. Figure 13 shows a comparison of a GPS snapshot RAIM algorithm used to produce integrity and the HIGH algorithm in normal (fault free) operation. The integrated solution can actually provide integrity after complete loss of GPS data as shown in Figure 14. In Fig. 14, GPS inputs to HIGH were removed at time 0. A GPS receiver would have lost all integrity at time 0 as well.

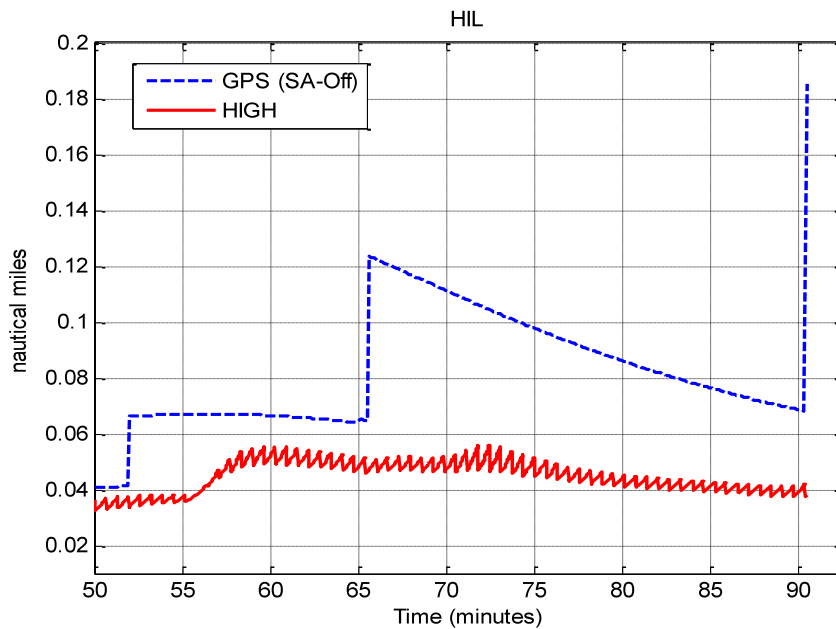
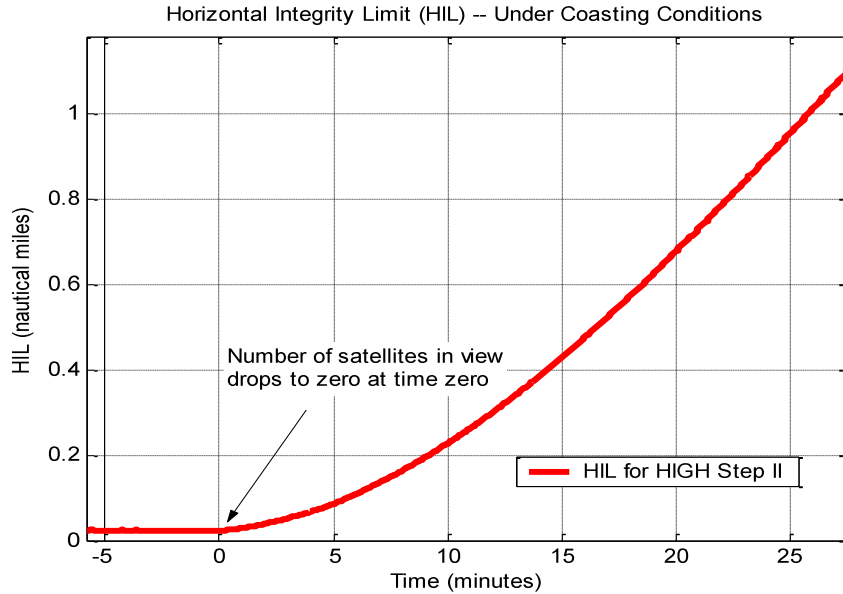


Figure 13

**Fig 14**

Continuity is improved by reduced sensitivity to integrity limit changes due to integrity coasting and the ability to isolate and exclude failed satellites once a failure occurs.

As the snapshot solution integrity changes abruptly in time as shown in Figure 13, there may be times when these changes exceed the required operational integrity (HAL). The integrity coasting provided by the integrated solution has a high probability of staying under the HAL and allowing the operation to continue to completion and therefore not affect continuity.

GPS outages that initiate coasting may occur with intentional or unintentional signal interference as well as satellite masking from the terrain or buildings such as the terminal. These coasting capabilities greatly enhance system continuity.

Fig. 15 demonstrates HIGH's ability to detect and exclude a low ramping failure while exposing the system to a RAIM hole. In this scenario, a 0.1 m/s ramping error is injected on the hardest to detect satellite at the same time the RAIM hole begins. If the system detects and excludes the failing satellite before the HAL limit is reached, the operation would continue to completion. This isolation capability makes the integrated system continuity less sensitive to certain types of failures.

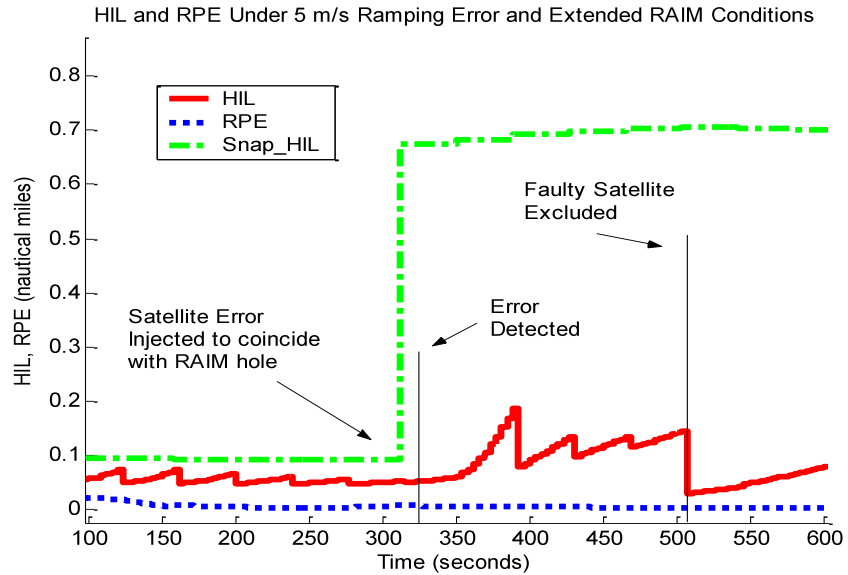


Fig 15

Availability is improved by the integrity coasting during periods of GPS loss or poor geometry. Fig. 16 shows HIGH’s HIL distribution versus the HIL distribution from a snapshot RAIM system (with calibrated pressure altitude) at the same instant in time with SA turned off. Tests for both systems used the 24 satellite almanac defined in DO-229 Appendix B with a 2 degree mask angle.

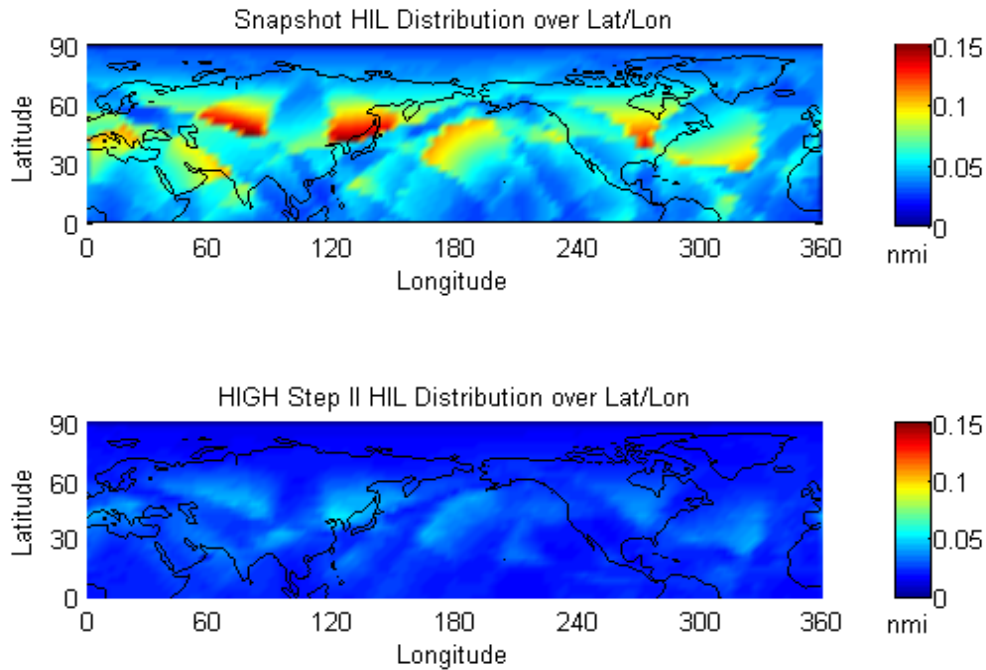


Fig 16

Conclusion

Accuracy, integrity, continuity and availability are common in any form of safety critical navigation system. As IMO requirements on navigation systems are adapted to the marine industry, integrated sensor architecture techniques and display methods similar to that employed by the aviation industry may be beneficial.

References

- [1] J. McDonald, Kendrick, Joshua. "Benefits of Tightly Coupled GPS/INS for RNP Operations in Terrain Challenged Airports," *Proceedings of ION-PLANS-2008, Proceedings of Position Location and Navigation*, Salt Lake City, UT, 2008.
- [2] Curt Call, Mike Ibis, Jim McDonald, Kevin Vanderwerf. "Performance of Honeywell's GPS/INS Hybrid (HIGH) for RNP Operations," *Proceedings of Position Location and Navigation Symposium-2006*, San Diego, CA, 2006.
- [3] RTCA Document No. RTCA/DO-229D, *Minimum Operating Standards for the Global Positioning System / Wide-Area Augmentation Systems Airborne Equipment*.

Contact Information

Mark Ahlbrecht, Staff Engineer
Honeywell Aerospace
Guidance and Navigation
8840 Evergreen Blvd, MN51-1305
Coon Rapids, MN 55433-6040

mark.ahlbrecht@honeywell.com

(+1) 763-957-4322