High Integrity Positioning: Lessons from the Aviation Industry

Marine Technical Society
Dynamic Positioning Conference
October 12, 2010

Mark Ahlbrecht

Honeywell

Return to Session Directory

Introduction

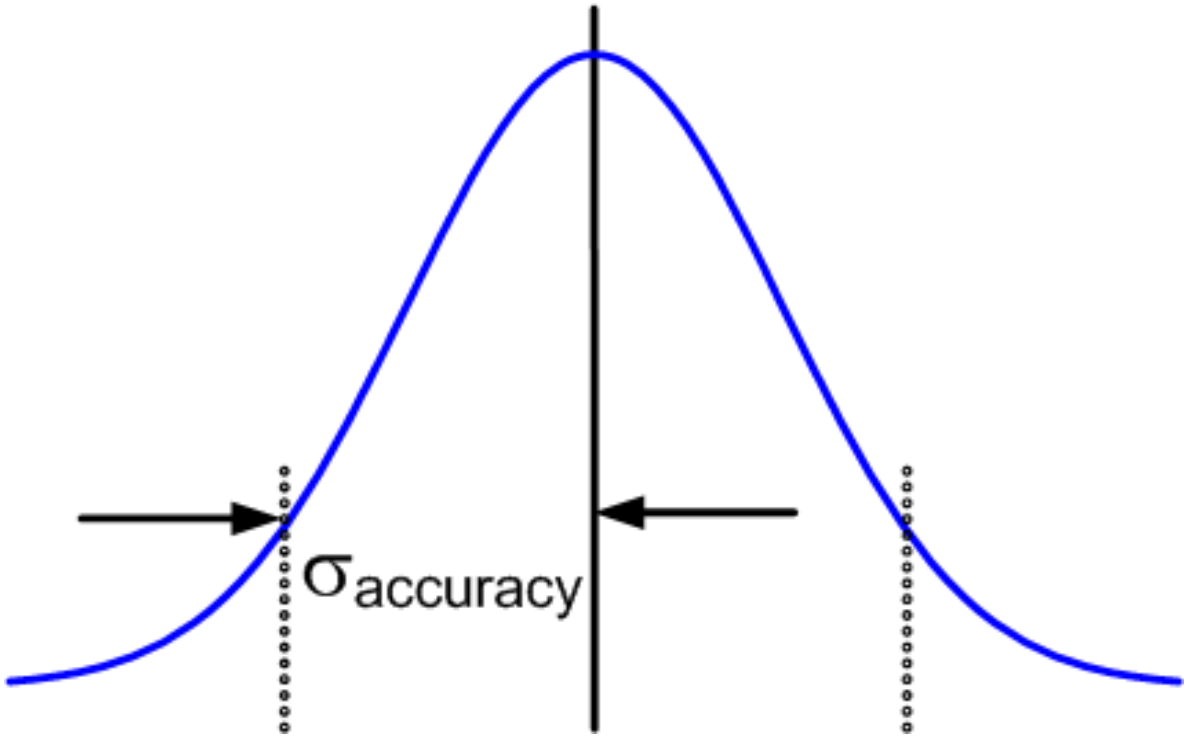
Honeywell

- Navigation positioning systems requirements:
  - Accuracy
  - Integrity
  - Continuity
  - Availability
- Difficult trade-offs when high integrity is required
  - Critical phases of flight
  - Dynamic positioning
- Integrated architectures offer advantages for safety
- INS/GNSS Hybrid integrated architecture (HIGH) is an example.

Accuracy

Honeywell

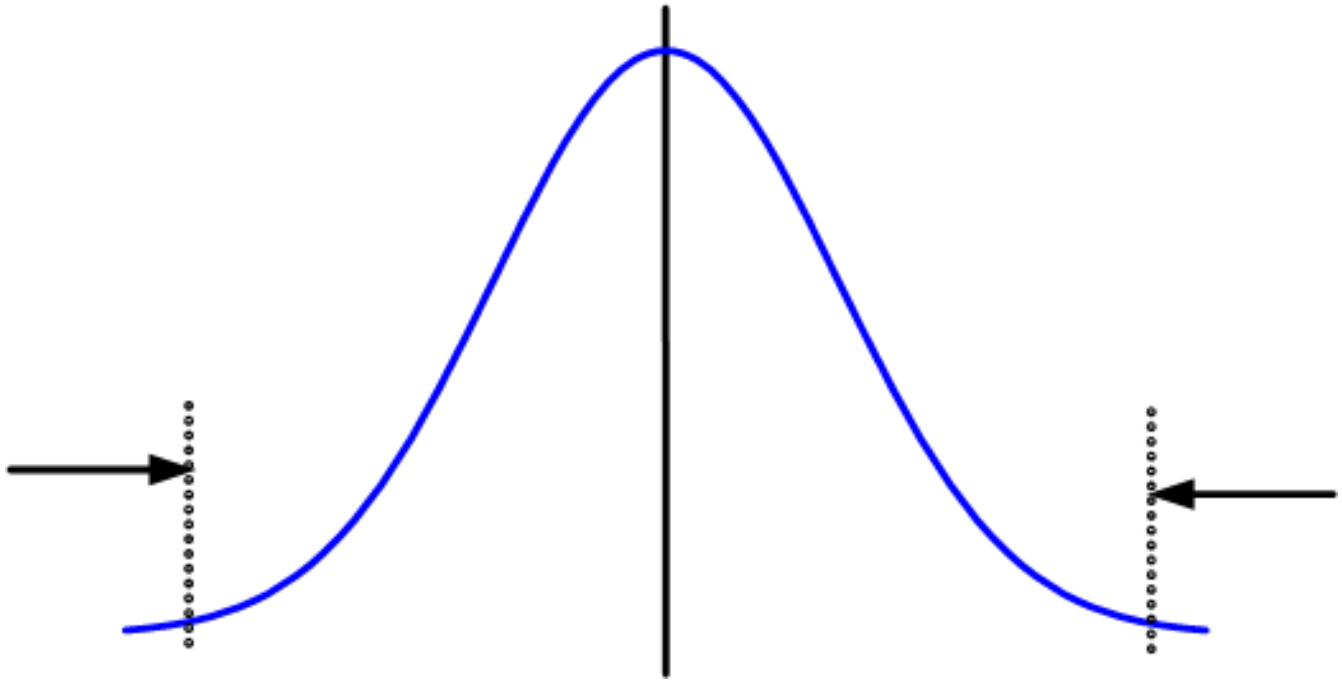
- Difference between measured and actual position
- Defined in a fault-free condition



Accuracy

Honeywell

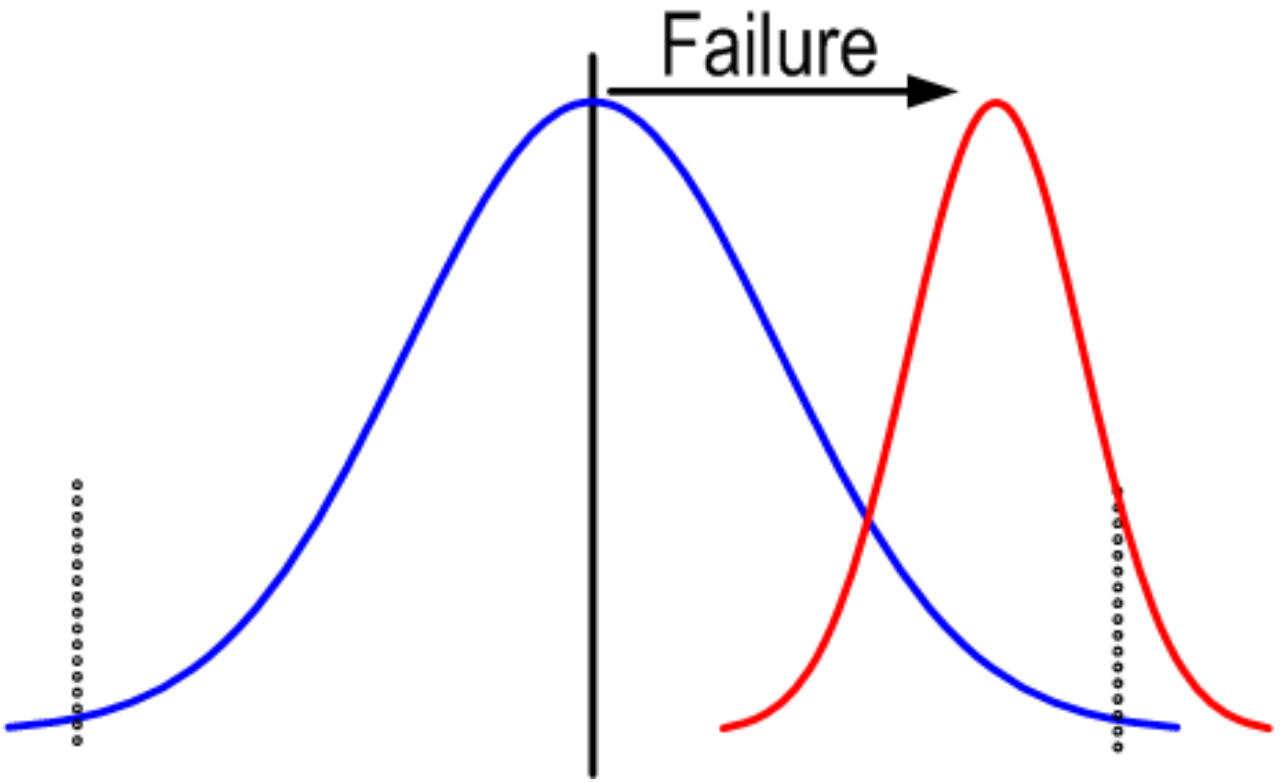
- Difference between measured and actual position
- Defined in a fault-free condition



Accuracy

Honeywell

- Difference between measured and actual position
- Defined in a fault-free condition



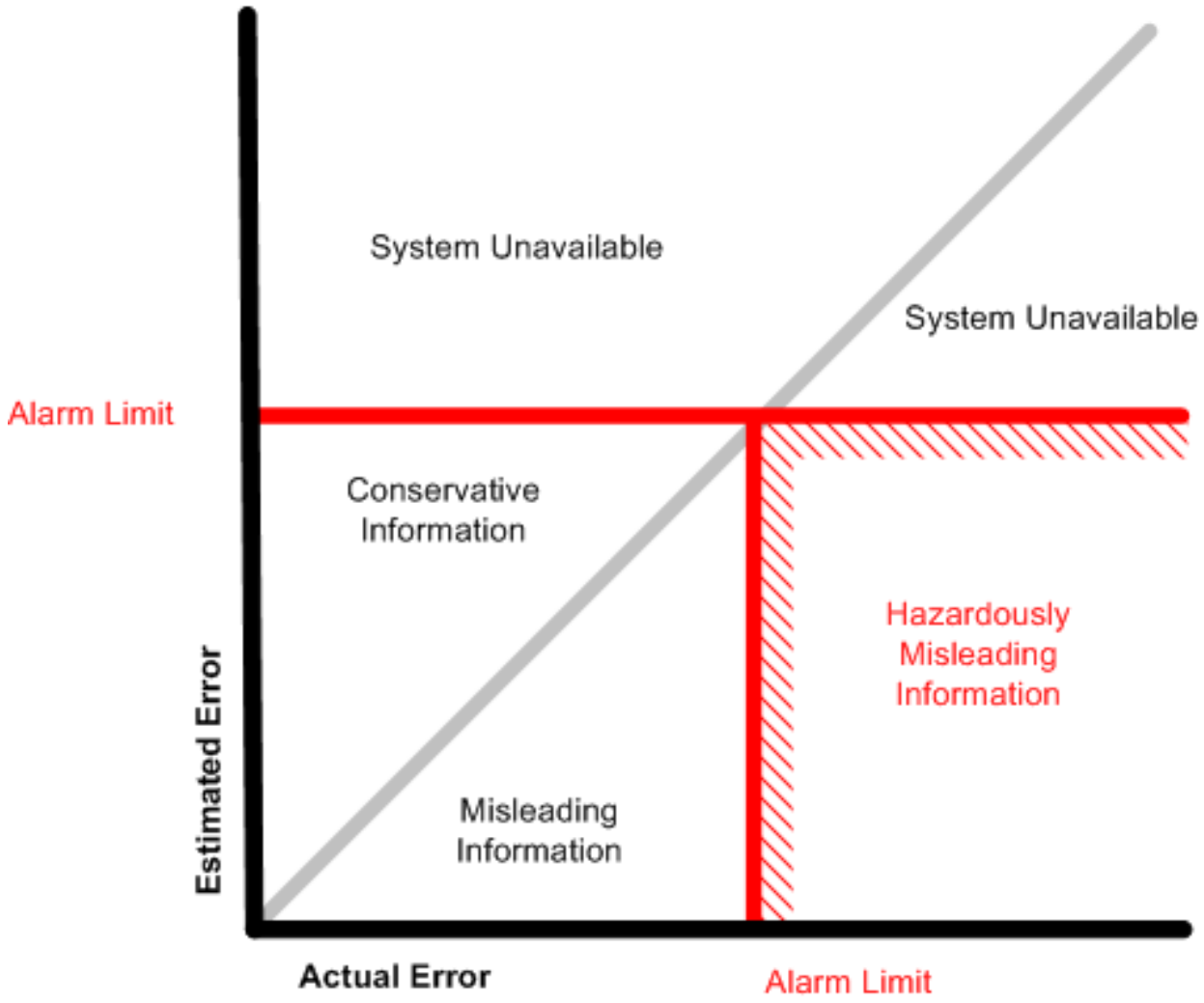
Integrity

Honeywell

- Provide timely warnings when the system should not be used for navigation
- Components:
  - System Estimated Error
  - Maximum Allowable Error (Alarm Limit)
  - Minimum Time to Alarm (TTA)
- Specified as the Probability of Hazardously Misleading Information (HMI)
  - P([Actual Error >= Estimated Error AND …
    Actual Error >= Alarm Limit]
    for greater than the TTA)
- Includes undetected failure scenarios

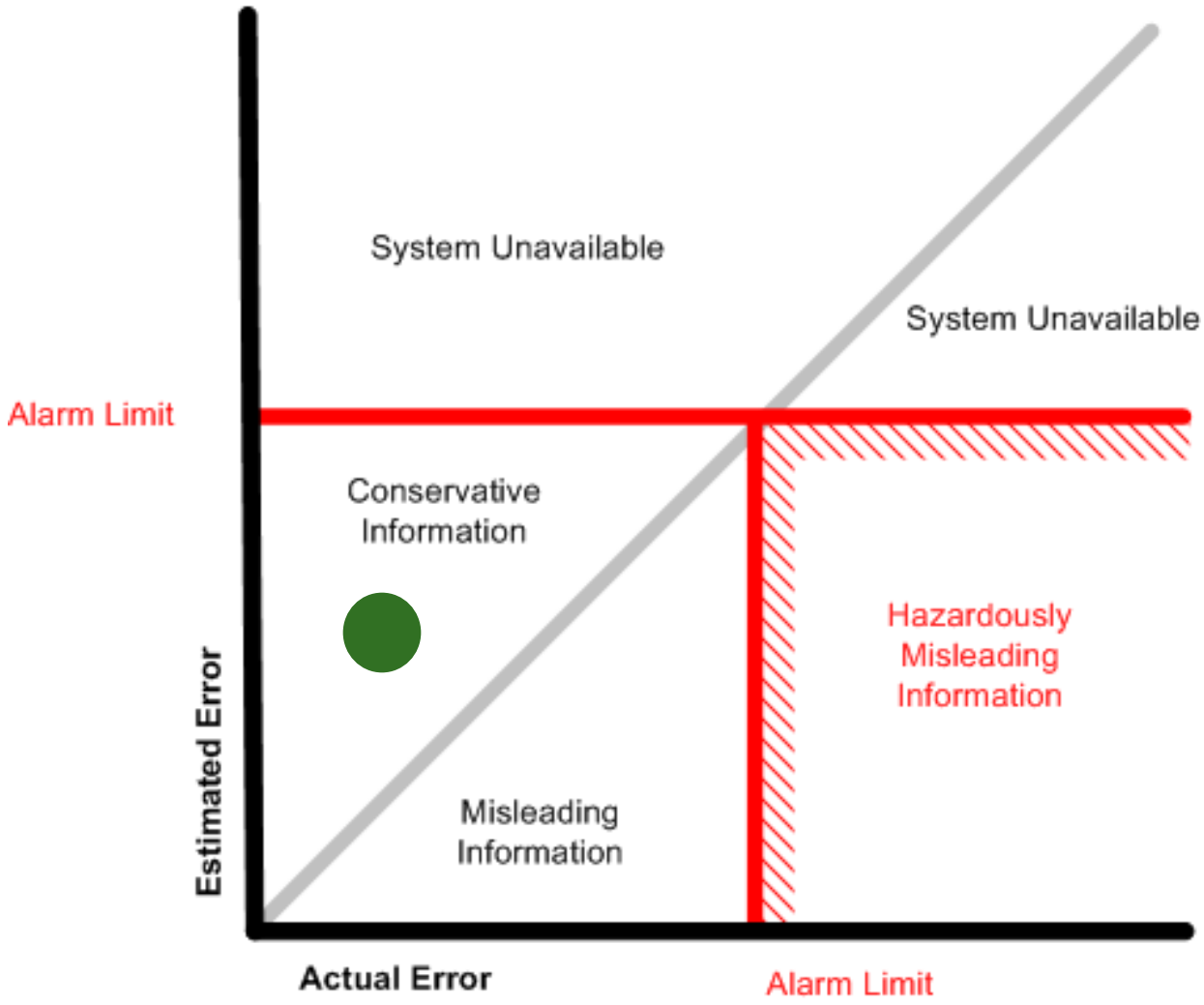
Integrity

Honeywell



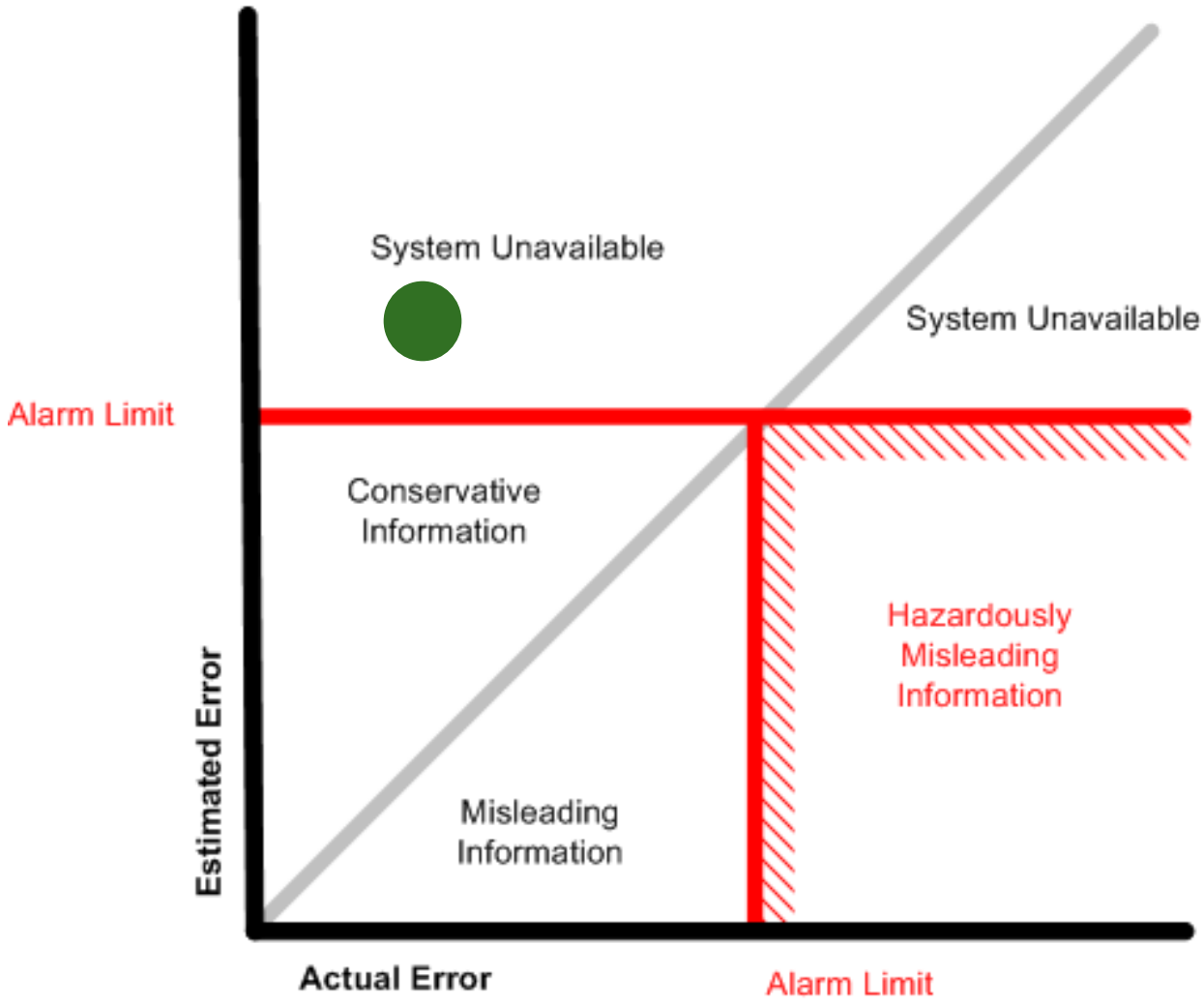
Integrity

Honeywell



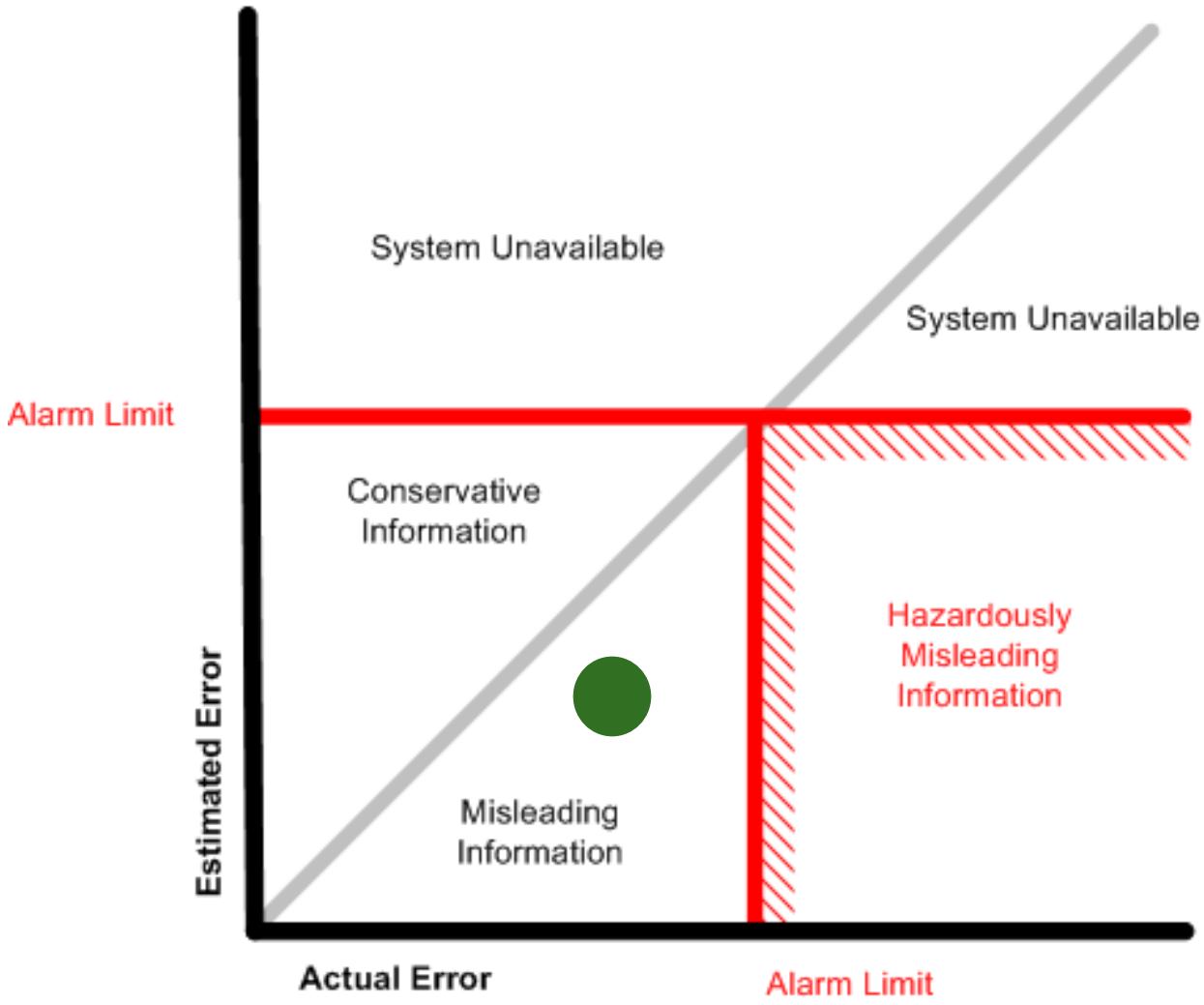
Integrity

Honeywell



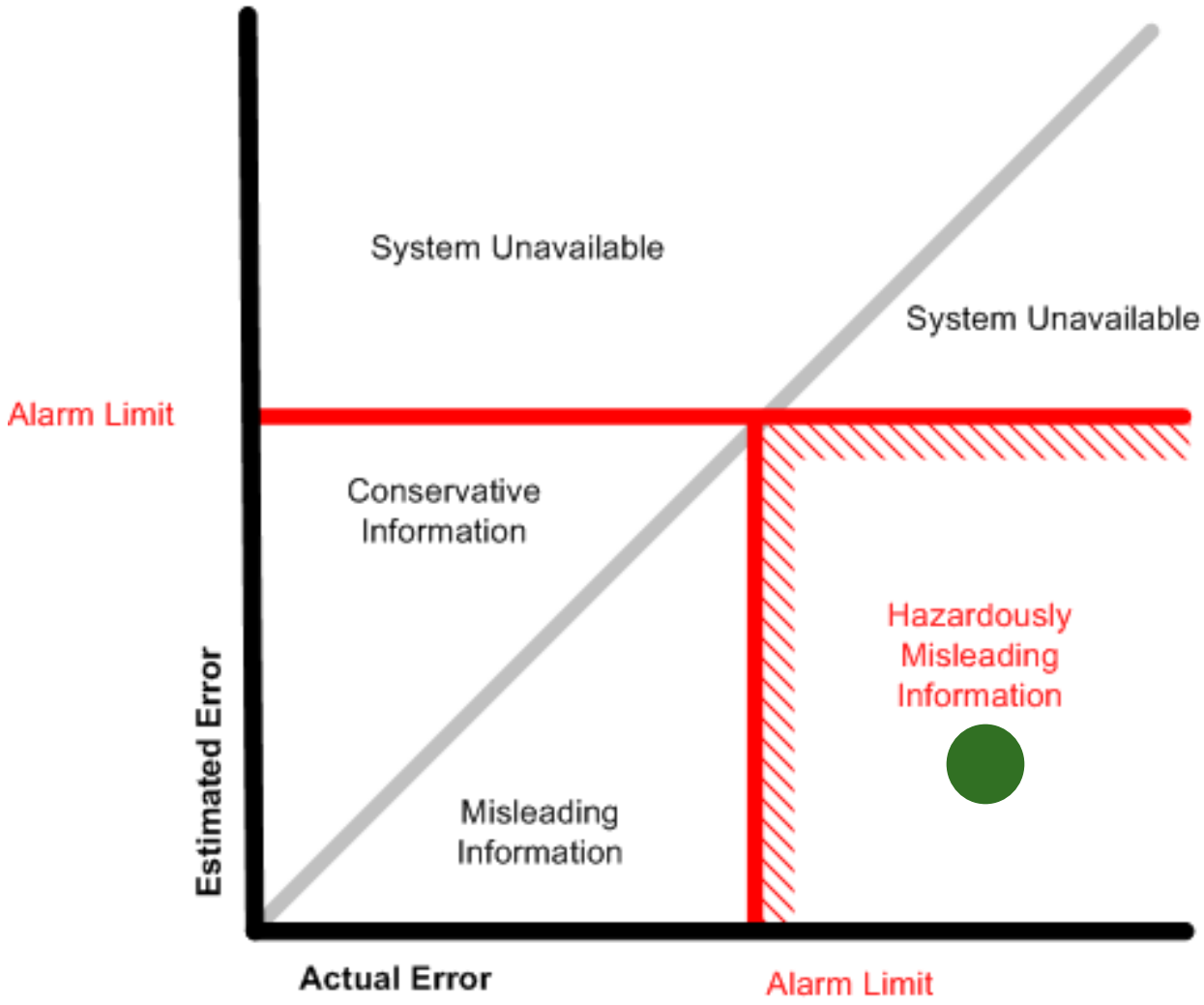
Integrity

Honeywell



Integrity

Honeywell



Horizontal Integrity Limit

Honeywell

- The Horizontal Integrity Limit (HIL) is the region of protection at the required integrity, given an undetectable failure is present
- Guidance equipment can use the HIL output by the system and compare it to the Horizontal Alarm Limit (HAL) required by the operation
  - If the HIL < HAL then operation continues
  - If the HIL >= HAL then the operation aborts

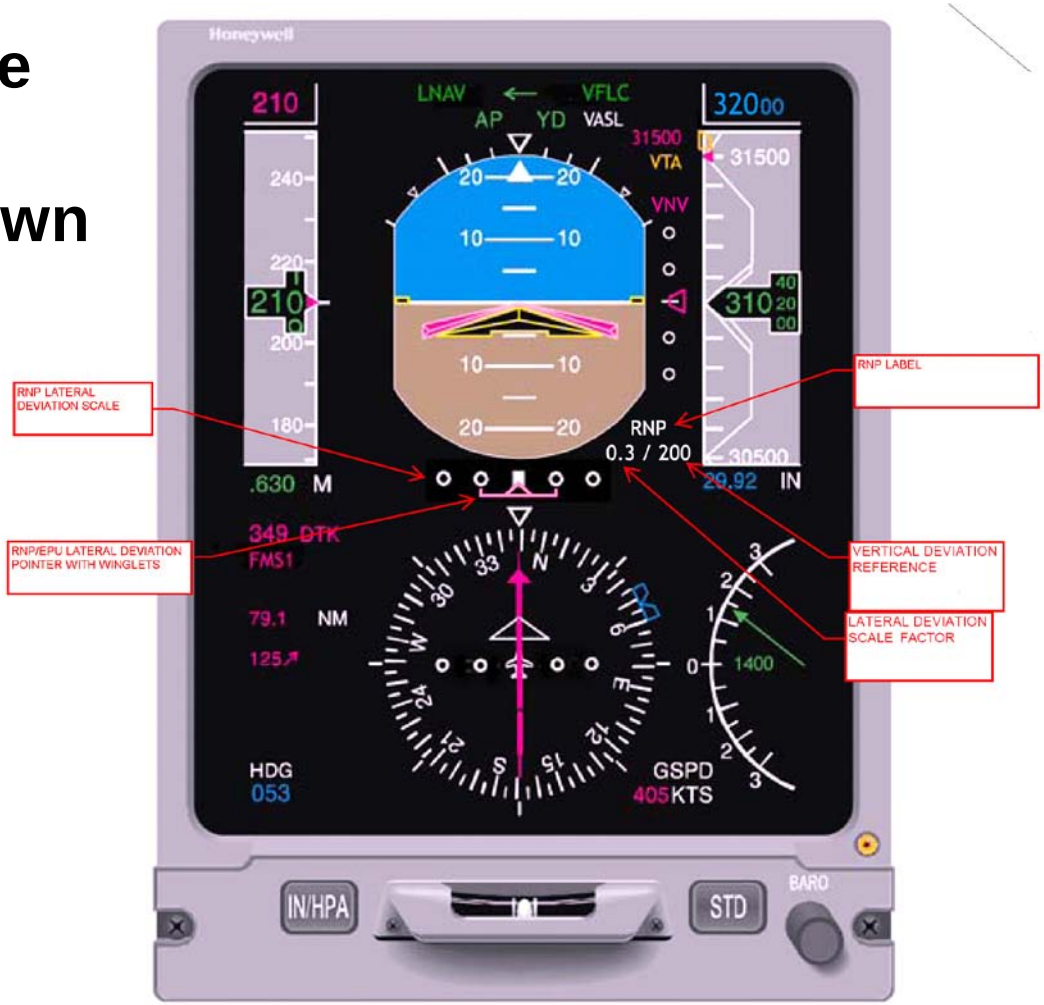
Integrity User Interface

Honeywell

- Required operational integrity is known to the user (HAL)
- Current integrity is known by the system (HIL)
- A user interface communicates the integrity status

- Continue Operation

- Abort Operation



Continuity and Availability

Honeywell

- **Continuity**
  - Probability that a valid navigation solution will be provided for the period of the operation
  - Aborting a high integrity operation has its own risks
- **Availability**
  - The percentage of time the system satisfies all of the accuracy, integrity, and continuity requirements at the start of the operation
  - Measure of the usability of the system as a whole

Aviation Requirements

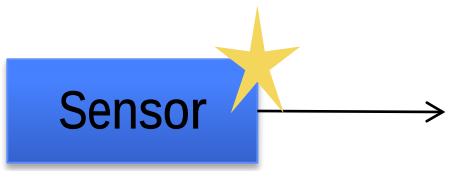
Honeywell

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	$2x10^{-7}$ / 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	1.8x10-6/ 15 sec	1.8x10-6/ 15 sec
Availability	0.99 – 0.99999 %	0.99 – 0.99999 %	0.99 – 0.99999 %	0.99 – 0.99999 %	0.99 – 0.99999 %

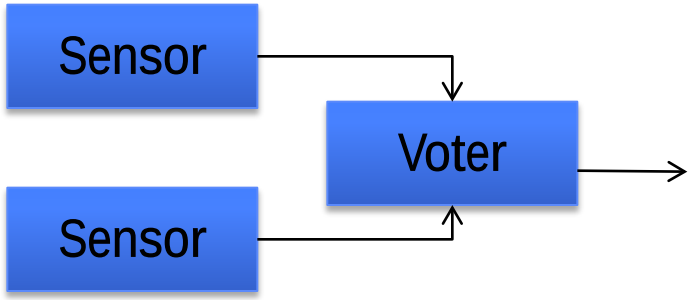
High Integrity Architectures

Honeywell

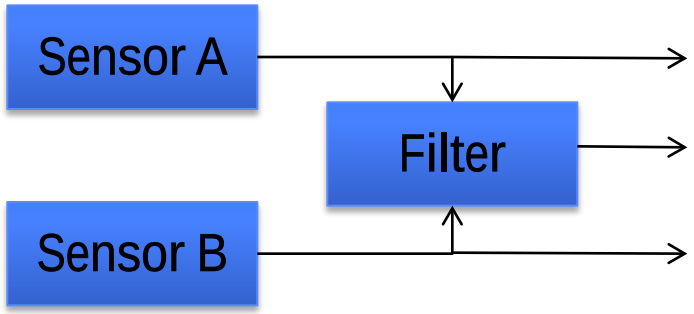
- **High Reliability**
  - Can be costly
  - May not be an option (GNSS)



- **Redundant**
  - Cost for duplicated function
  - Increased continuity/avail
  - Voter adds new failure modes

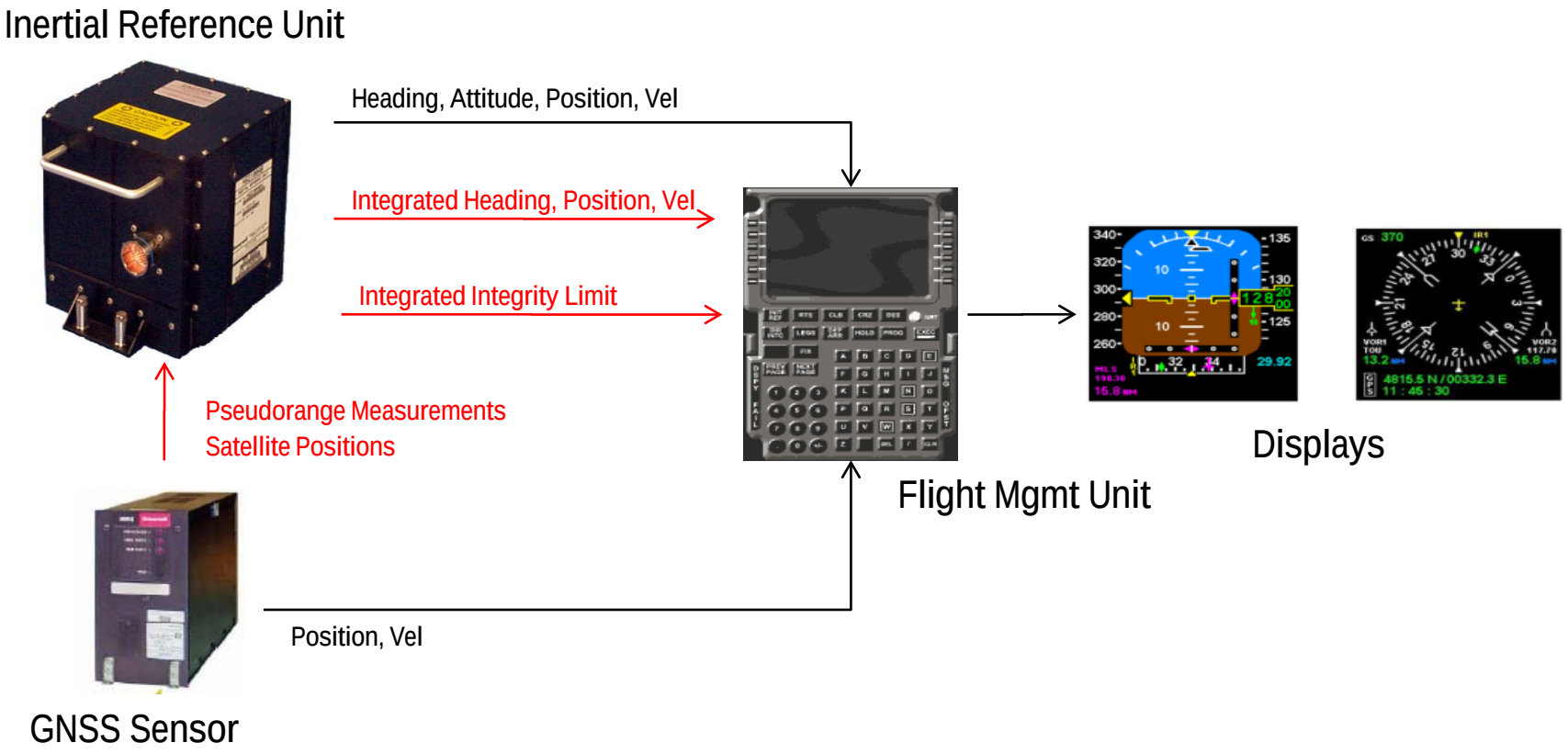


- **Integrated**
  - Fuse complementary safety properties
  - Increase continuity/avail
  - Can be complex



High Integrity IRU/GNSS Architecture

Honeywell

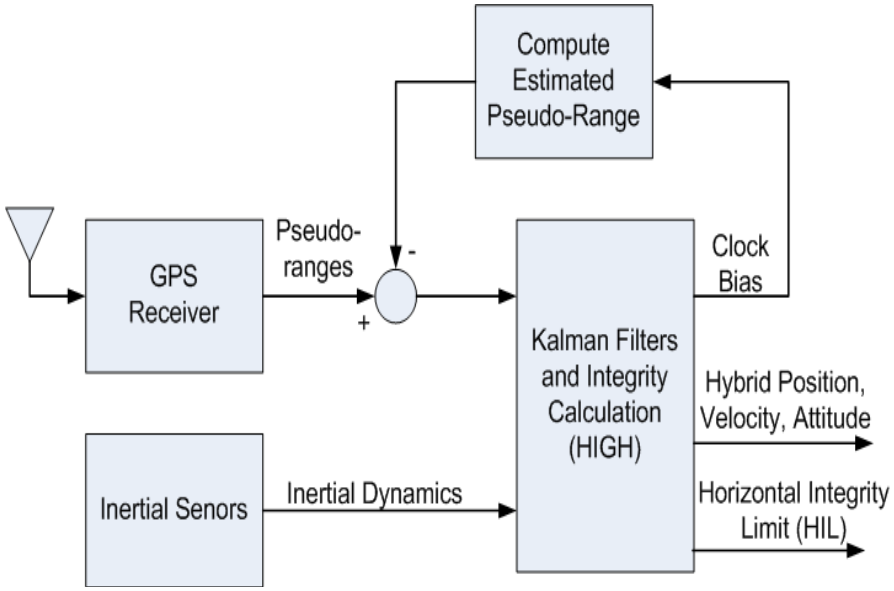


- **By sending GNSS data to the IRU it is possible to form:**
  - **an integrated navigation solution, and**
  - **integrated integrity**

Integration Method (HIGH)

Honeywell

- **Kalman Filters**
  - Used for years
  - Sensors with complementary properties
- **Advantages**
  - Fused accuracy
  - Fused bandwidth
  - Fused integrity
- **Honeywell INS/GPS Hybrid (HIGH)**
  - Uses multiple Kalman filters
  - Examines separation between filter solutions



Impact of Satellite Errors on Hybrid Systems

Honeywell

- **Kalman filters within a hybrid system can be corrupted by satellite errors.**
  - **Typically Ramps or Steps in Pseudo-Range**
- **Once a Kalman filter has been affected by a satellite error, the impact of the error cannot be removed**
  - **This has a major impact on integrity.**
- **Advantage of using solution separation as an integrity scheme is that there is always a fault-free solution**

HIGH Allows Operations Even After a Satellite Failure

Solution Separation Method Description

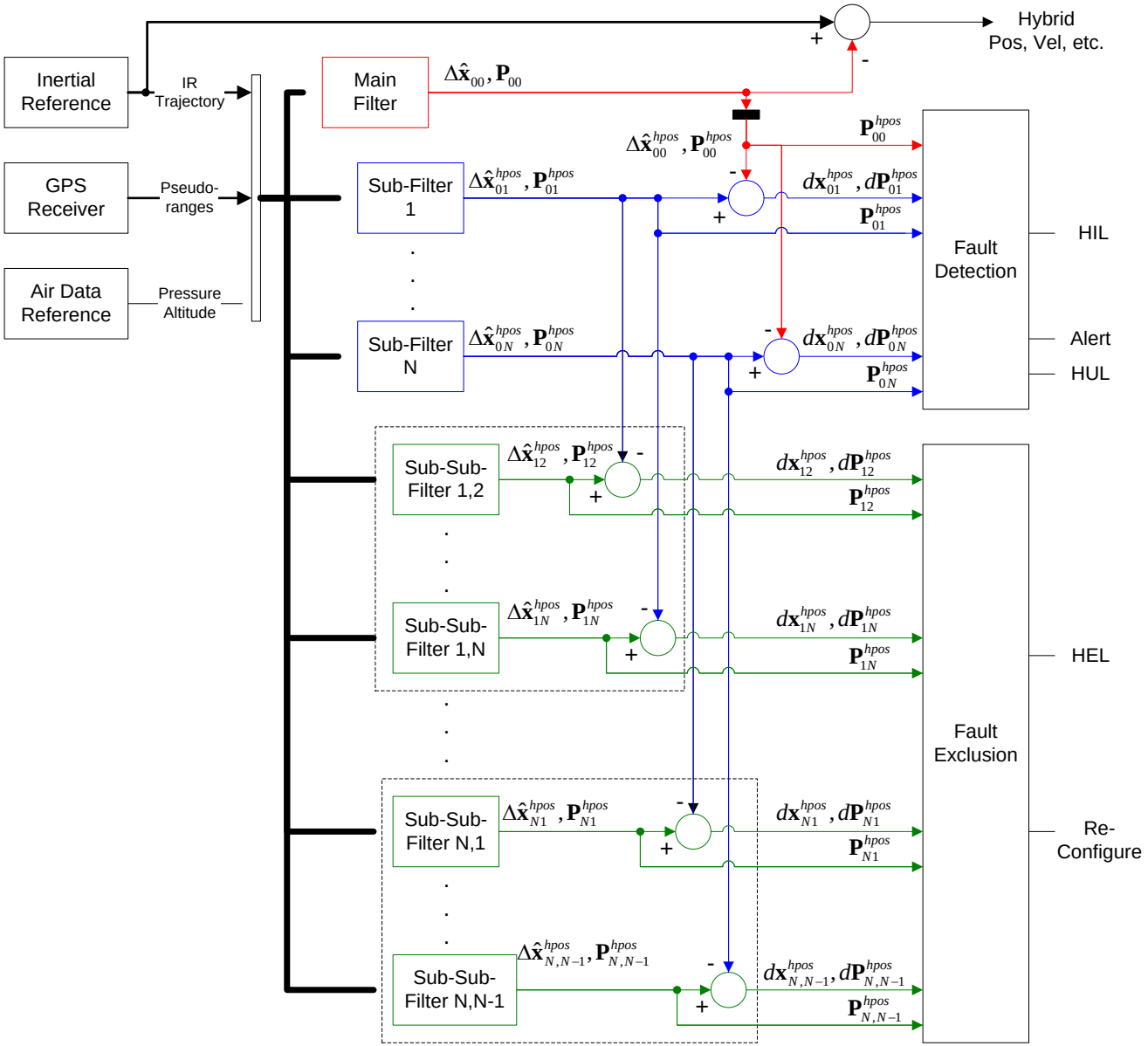
Honeywell

- **HIGH Step II Maintains a Bank of Kalman Filters**

Main Filter	(uses N satellites)
Sub-Filters	(use N-1 satellites)
Sub-Sub-Filters	(use N-2 satellites)

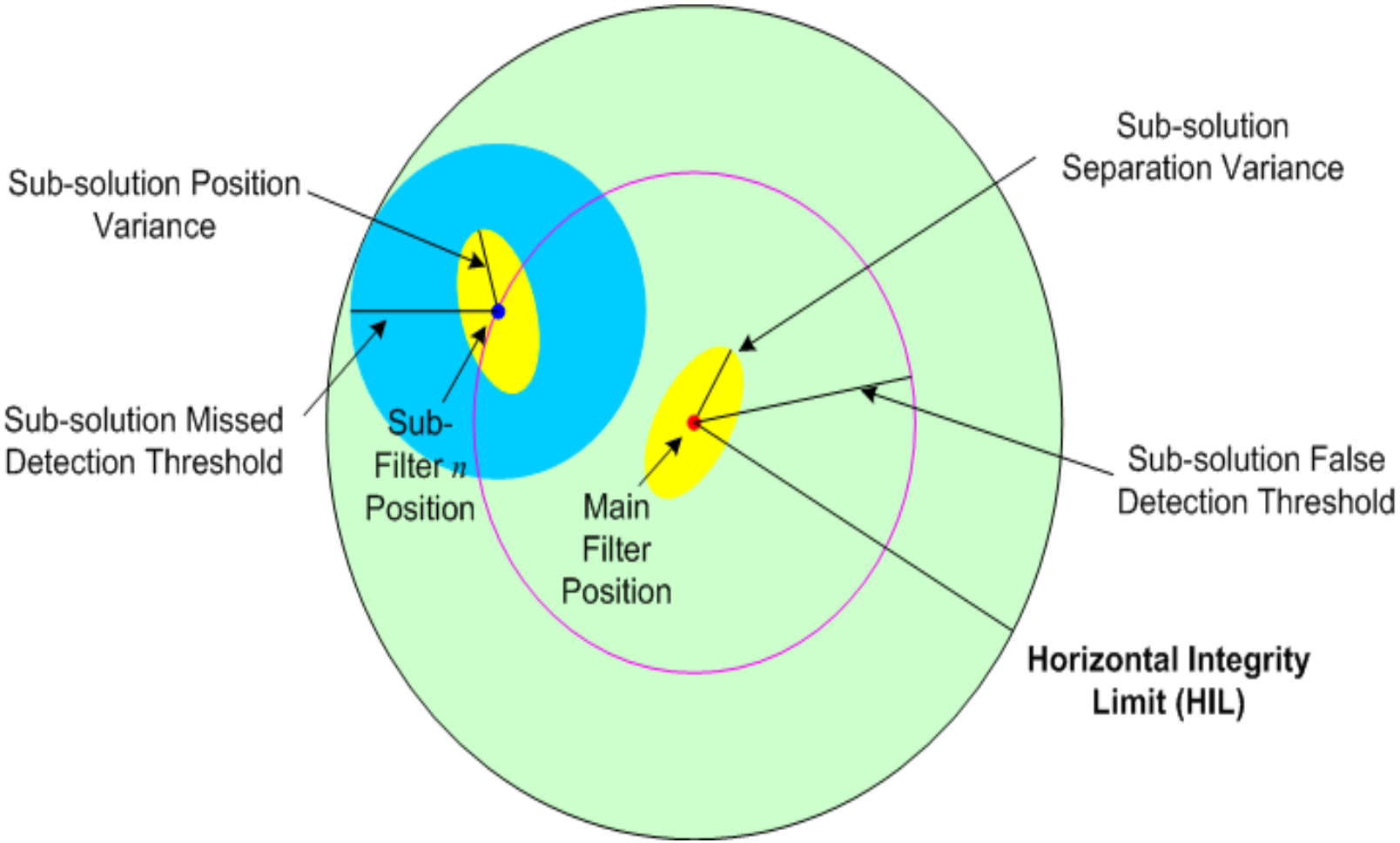
HIGH Implementation of Solution Separation

Honeywell



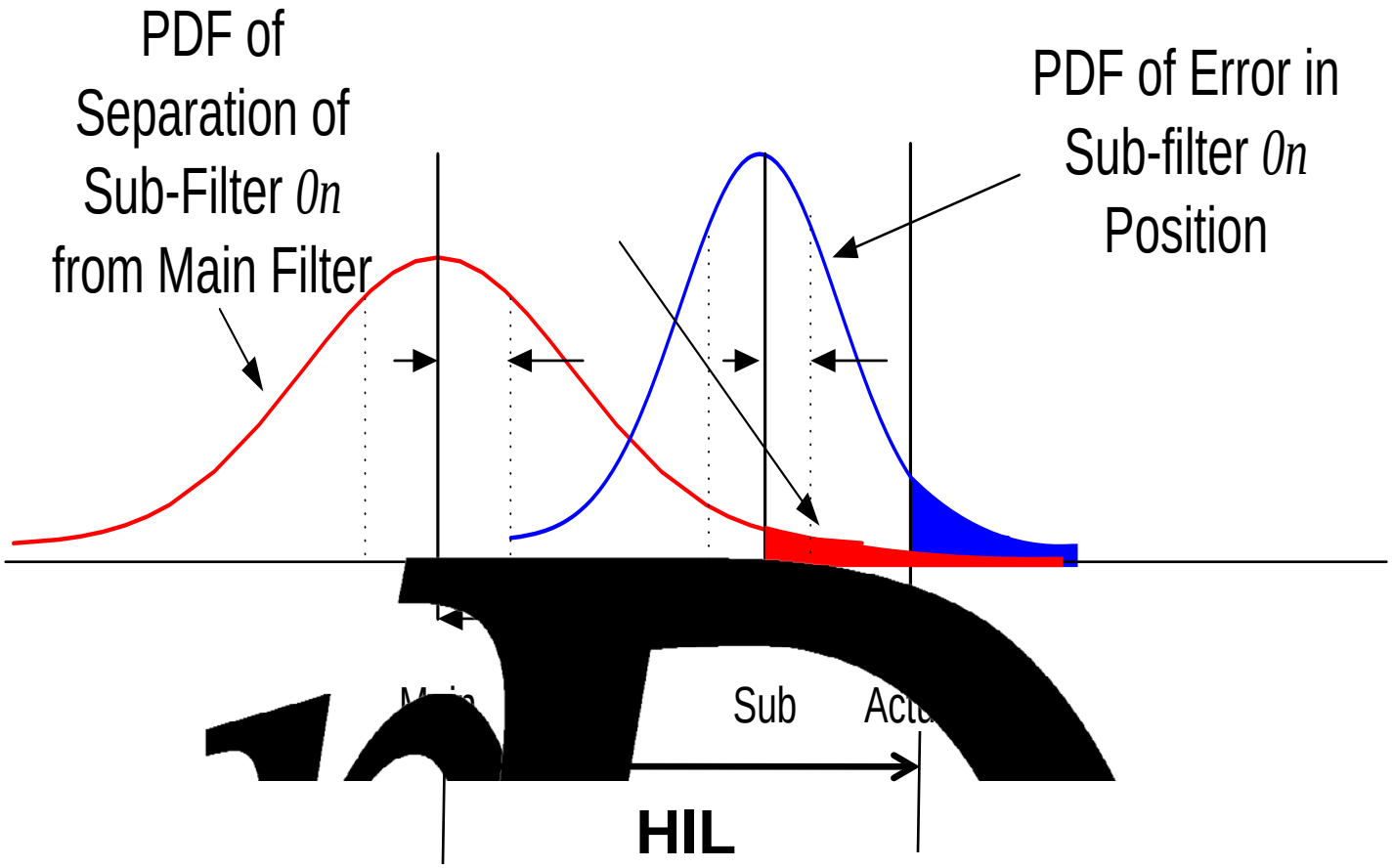
Calculation of Horizontal Integrity Limit

Honeywell



Calculation of Horizontal Integrity Limit

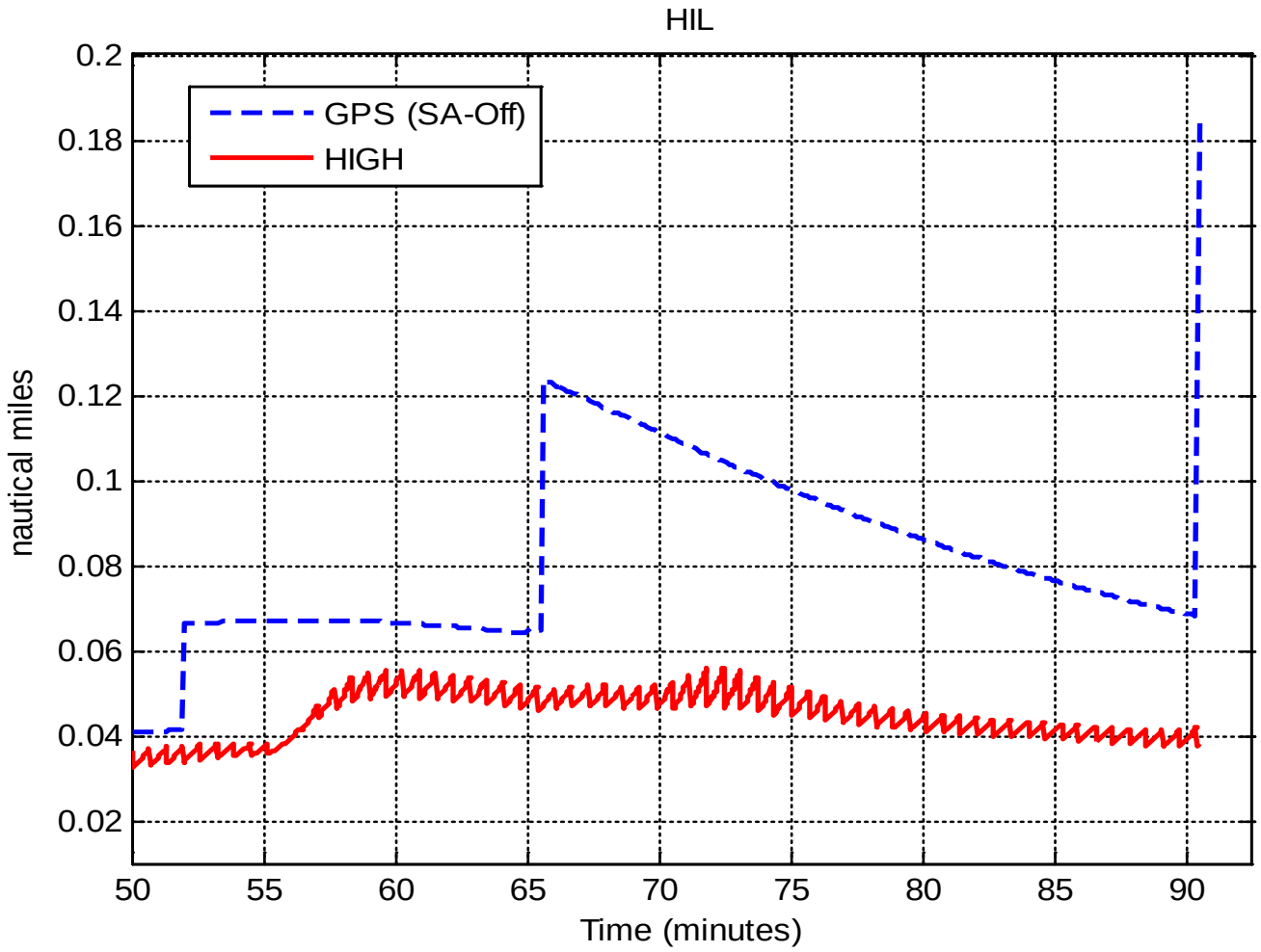
Honeywell



- **Another way to think of HIL is the position bound at the time of detection**

Integrity Coasting Performance During Nominal Test

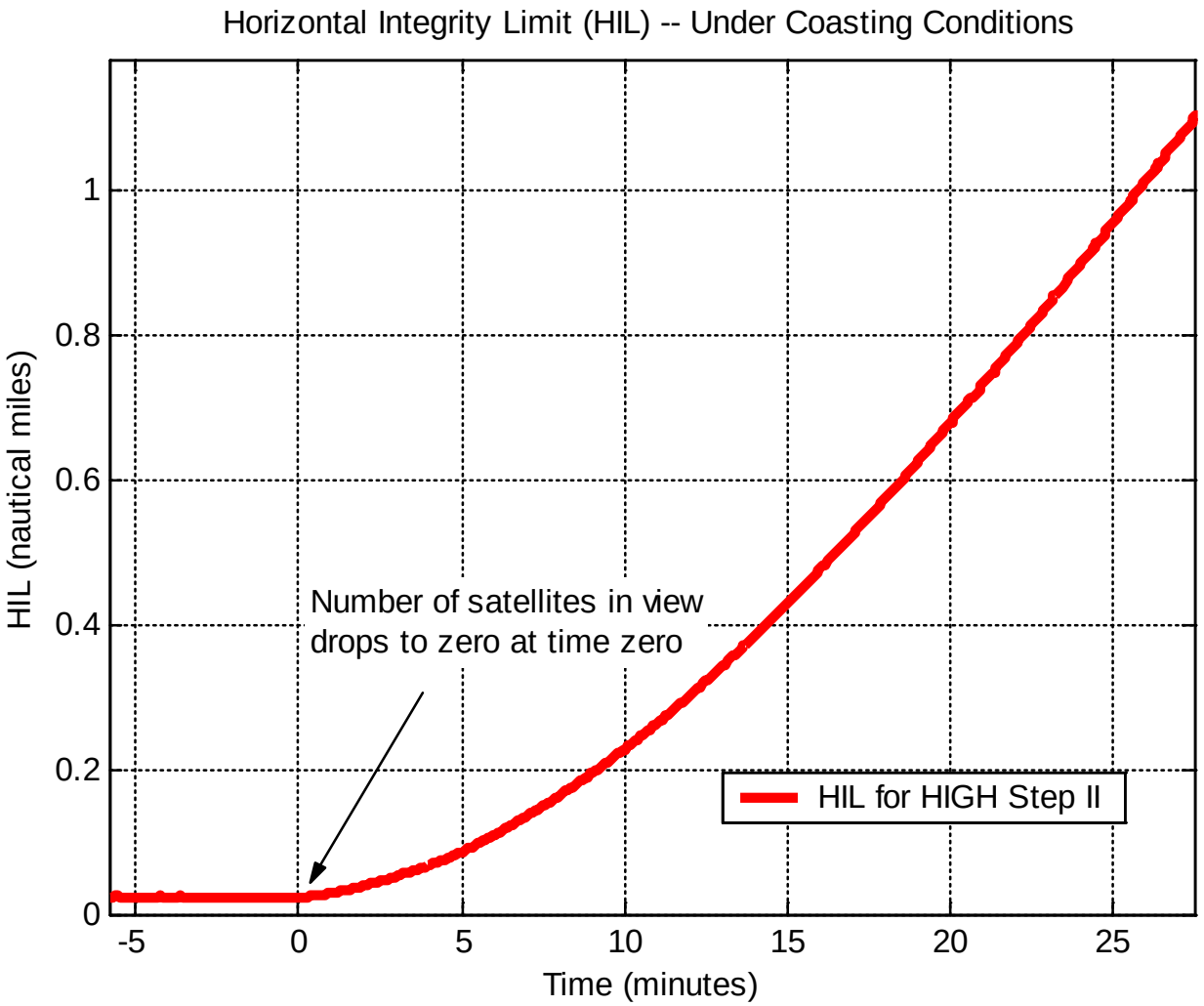
Honeywell



HIGH Less Sensitive to Satellite Geometry and Masking

Integrity Coasting Performance During Flight Test

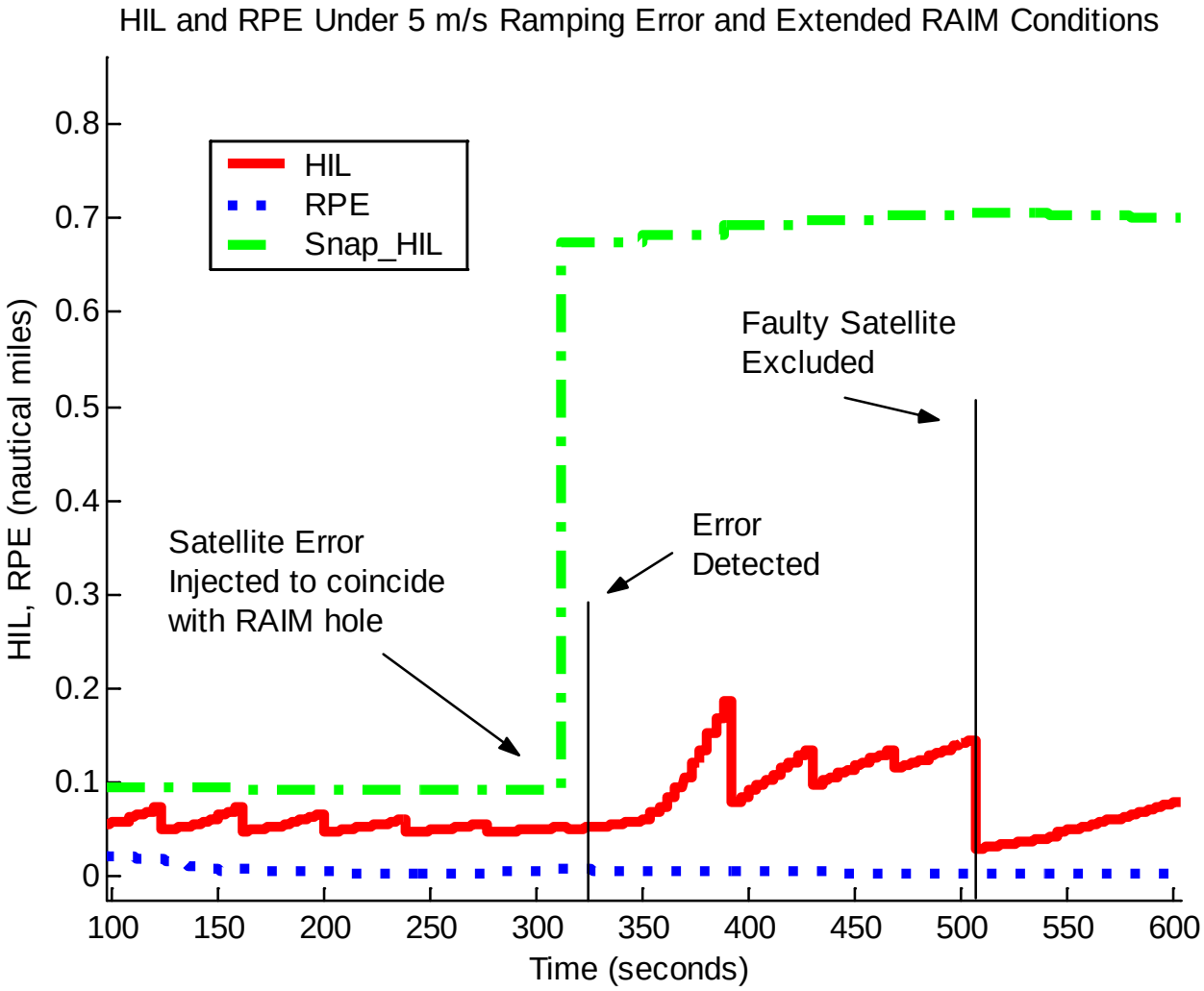
Honeywell



HIGH Provides Integrity Even After GNSS Loss

Fault Detection and Exclusion

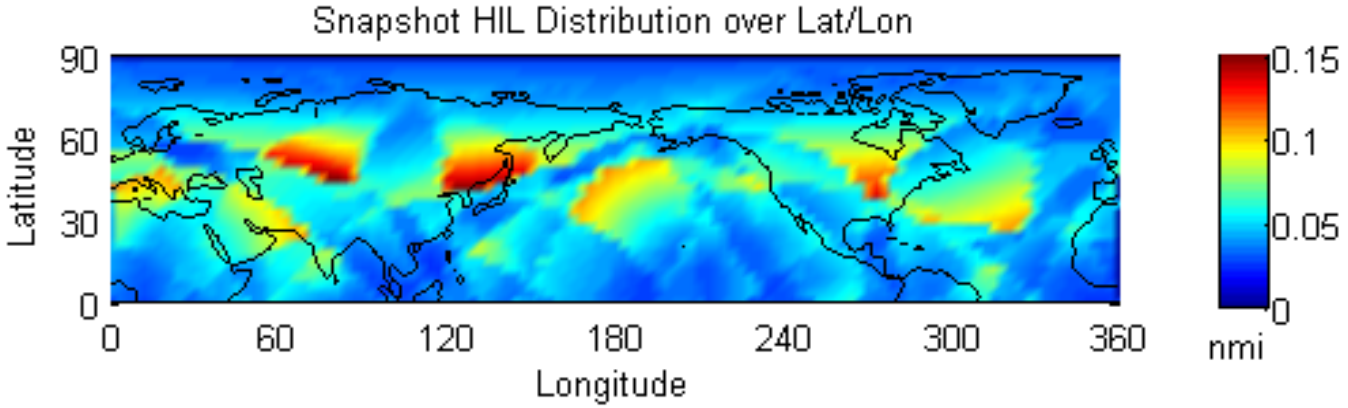
Honeywell

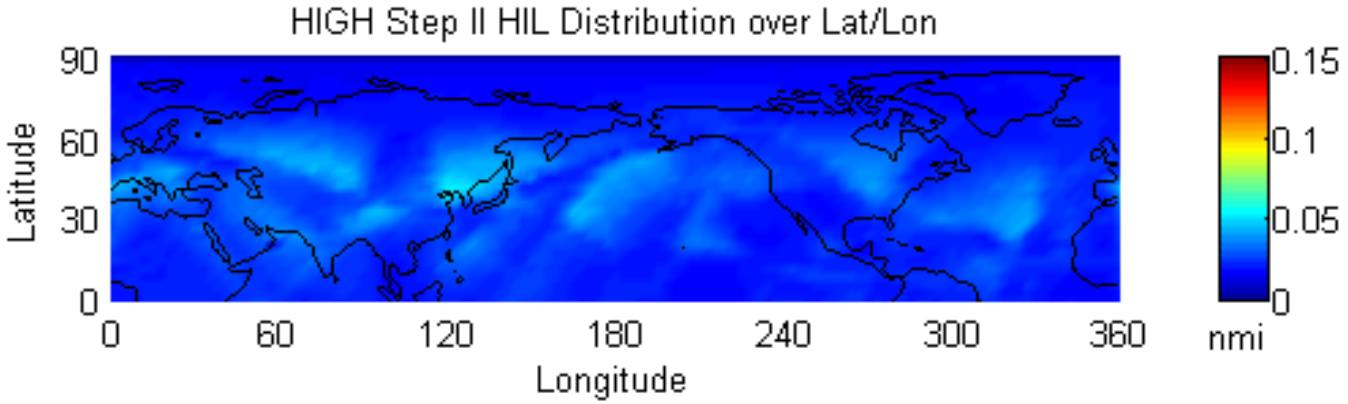


HIGH Provides Fault Detection/Exclusion in Poor Geometry

Time Slice for HIGH Availability

Honeywell





HIGH Improves Availability

Conclusion

Honeywell

- Accuracy, integrity, continuity and availability are common needs in any form of safety critical navigation
- IRU/GNSS integration with solution separation provides advantages:
  - Lower integrity limits under both nominal and adverse geometries
  - Higher availability
  - Operations even after a satellite failure
  - Integrity even after satellite dropouts
  - Fault detection and exclusion even in poor geometry

Thank You!

Mark Ahlbrecht
Honeywell Aerospace
mark.ahlbrecht@honeywell.com
+1 763-257-2386

Honeywell