GPS is by far the best-ever system for both navigation and timing. Recognition of that is essentially universal. Less widely recognized are the ramifications of growing dependence on GPS, in both communications and navigation. This discussion will concentrate on the latter, highlighting attendant risk in flight. Although extensive deliberation already exists, I'll presume to offer my experience. Immediately it is acknowledged that the risk is low; but now let's ask what is low enough. While every effort is made here to avoid an alarmist tone, answering that question calls for an unflinching look at potential consequences if the gamble ever failed.

It is insufficient to argue that no system is perfect; clear perspective calls for some quantitative measure. To approach that without undue complexity, consider an example with 3000 airliners, each averaging two landings per day, at one-in-a-million chance for a navigation-induced accident. We could then expect two mishaps per year from navigation. With 50,000 global flights daily, change that two per year to seventeen. Unacceptable as that is, it only begins to address the overall scope of this issue. GPS lives up to expectations, brilliantly performing as advertised. Even that best-ever performance must (and does) have tolerance for occasional error – examples, though rare, are documented. To live with less-than-perfect performance, the industry relies on integrity testing (wherein comparison checks using extra satellites can detect inconsistencies and exclude questionable data). Methods are firmly established and supported by widely documented successful results.

Existence of sophisticated methods supported by accumulated experience – now over a period of decades – can create perceptions of a fail-safe system. Alas, complacency calls to mind the Titanic's lifeboats, plus a statement originating with the author of The Peter Principle (regarding people promoted to their level of incompetence)

When fail-safe systems fail, they fail by failing to fail safe.

Reasons for caution are largely obscure but valid. Despite wide and fully earned acclaim for the excellent 2001 Volpe report, commitment to a key means of backup for GPS is very incomplete. To ensure that the danger of a disaster is fully realized, a painful look must show some very inconvenient facts. They are reviewed here as succinctly as thoroughness allows.

- There is no standard integrity test; suppliers are allowed to devise their own validation methods.
- That may have worked when life was simpler. Life is no longer simple –
  http://jameslfarrell.com/wp-content/uploads/2010/05/robust.pdf.
  http://jameslfarrell.com/wp-content/uploads/2010/05/gnss09.pdf
- Standardized blind testing (wherein those performing the test do not know the correct answers) was proposed *but rejected* by the collective will of the Fault Detection / Fault Isolation/Exclusion (FDI/FDE) Working Group for RTCA SC-159 (GPS Integrity).

A 1994 paper (ION-NTM, January 1994) from that Working Group, coauthored by Ohio Univ. Prof. Frank vanGraas (chairman) and myself (co-chairman), advocated rigor in several areas of validation. Special attention focused on real-world experience produced the common-sense prescription,

> "Retest: – if the equipment being tested fails, equipment must be modified to correct the problem before re-testing ... ."

The following tract from RTCA Paper No. 455-93/SC159-463 was highly instrumental in rejection of the test plan just described:

> "If a properly designed receiver fails the test, the manufacturer is required to modify or correct this receiver before retesting ... . This does not make sense: the receiver is, after all, designed properly, so what can the manufacturer `modify' or `correct'? "

The self-evident flaw in this reasoning is, of course, that a receiver *whose only outward indication is failure of a test* is still automatically assumed to be properly designed. Nevertheless, insufficient requirements were prescribed for end-to-end testing (from *r-f* in to final output). Furthermore, even the software verification relies largely on pseudocode (for *integrity*; note the irony).

Response to those events included a June 1995 communication from R. Lilley (former head of Ohio University Avionics Engineering Center) to RTCA's Tech Management Committee, advocating evaluation of test results "without commercial pressure affecting the outcome" and a subsequent letter-to-the-editor of the ION Journal (Winter 1997-98, page 497). That letter was written to by the FDI/FDE Working Group co-chairs.

Persistent doubts, expressed in that IONJ letter, were later vindicated in an independent investigation by Nisner and Johannessen ("Ten Million Data Points from TSO-Approved GPS Receivers: Results of Analysis and Applications to Design and Use in Aviation," *ION Journal*, Spring 2000). Extensive tests performed on certified receivers missed integrity performance goals by *four orders of magnitude*. Shortly thereafter, before the Legal Issues Panel at ION-GPS 2000, the following documented question was submitted:

> "*Given the awareness of this situation as well as the existence of documentation providing an example of misinterpreted certification test procedures, what are the liability implications for FAA, for the airlines, for the airframe manufacturers, and for the equipment suppliers in the event of an accident ?* "

The fact that no answer was recorded is also documented on page 1420 of *ION-GPS 2000 Proceedings*. The documented misinterpretation just mentioned refers to the first-ever certified receiver, now well known to have failed spectacularly in multiple facets of integrity testing by another manufacturer. It is readily acknowledged that correction of those early problems is quite credible, but one issue is inescapable: Historical proof of flightworthiness improperly bestowed – with proprietary rights accepted for algorithms and tests – did happen, and that was not widely known until much later.

Points just described were disseminated on the fifth page of a 2004 manuscript,
http://jameslfarrell.com/wp-content/uploads/2012/03/GPSfix.pdf .

There is still more. Efforts to obviate GO/NO-GO testing limitations also failed to gain committee approval. Consider a test with N maximum allowable missed detections – irrespective of whether each may be a near-miss or a *blunder* – with this hypothetical outcome from a large number of trial runs for two receivers:

- RCVR #1 produces N missed detections, each occurring with errors exceeding allowable levels by orders of magnitude. Decision: *Accept*
- RCVR #2 produces $N + 1$ missed detections, each occurring with errors exceeding allowable levels only slightly. Decision : *Reject*

That deficiency in acceptance criteria remains. A proposed quantifictation of integrity error was dismissed.

We can bend over backwards to acknowledge that disaster is unlikely, but the point here is that "unlikely" isn't good enough. The unflinching look at consequences noted near the start of this communication will now be exercised: Recall the meaning of ***G*** in ***GPS***. Imagine hundreds of aircraft, carrying receivers validated by good-but-not-perfect integrity tests, all within the region sighting a flawed satellite whose position provides desirable geometry while some other satellites are not helpful to various users (due to outages, track loop interrupt, multipath, blockage, geometry, sub-mask elevation, ...). There is no need to pursue the detailed results, except to say the stakes are so high that failures to detect with risks on that scale need to be unlikely in the *extreme* ; *wildly* improbable; *nowhere near* one in a million.

Presence of satellite-independent data for consistency checks, with appropriate scaling from error statistics, can enable detections otherwise unnoticed. Continued absence of this capability calls to mind the overconfidence of Amoco before Amoco-Cadiz, or Exxon before Exxon Valdez, or "best-and-the-brightest" economists acting with serene confidence until the 2008 financial fiasco.

All this is old information. Despite that, realization has not been widespread – and present plans for upgrading to Automatic Dependent Surveillance Broadcast (ADSB) raise new concerns (see the publication list, #83, plus various blogs on this site related to collision avoidance, runway incursions, •••). This dialogue is prompted by considerations of safety. Again, "low" likelihood combined with absence of a calamity thus far offers no guarantee. It is high time to address this issue with all its ramifications.