LORAN REVISITED (*written in March 2009 – see accompanying Blog*)

The recent OMB proposal to terminate Loran-C could be interpreted in either of two ways. i.e.,
- as an end to support for LF backup to GPS

or • as a step toward transition to eLoran.

As noted in a recent ILA communication, only the latter makes sense. In fact, this writer feels compelled to make a stronger statement: only the latter is at all rational. Despite the recognized importance of avoiding alarmist tones, a greater need is paramount in this instance – avoidance of dire consequences that could result from a brief lapse in operation with no backup. Only by an unflinching look at those consequences can the full impact be clarified.

GPS is by far the greatest system for both navigation and timing ever seen on this planet – recognition of that is essentially universal. Far less recognized are the subtle ramifications of growing dependence on GPS. It is insufficient to admit that no system is perfect; clear perspective calls for some quantitative measure. To approach that without undue complexity, an example is useful: consider a one-in-a-million chance for mishap. With 365 days in a year and over 3000 aircraft, each averaging four vulnerable flight phases (two takeoffs and two landings) per day, we could expect four mishaps per year from navigation. 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 have (and does have) tolerance for occasional error; examples of that, 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 to perform those tests are firmly established and supported by documented results.

Existence of sophisticated methodology supported by accumulated experience – now over a period of decades – can lead to perceptions of a fail-safe system. Alas, any such 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 this caution are largely obscure but very real. Despite wide and fully earned acclaim for the excellent 2001 Volpe report, commitment to a key means of backup for GPS is unclear. To ensure that the danger of a disastrous decision is fully realized, a painful look must highlight some very inconvenient and unperfumed 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.
- Standardized blind testing (wherein those performing the test do not know the correct answers) was proposed and 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 Farrell (co-chairman) and vanGraas (chairman), advocated rigor in several areas of validation. Special attention focused on obvious failures produced the following 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 the 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 <u>whose only outward indication is failure of a test</u> 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).

Letters written in response to those events included

- a June 1995 communication from R. Lilley (former head of Ohio University Avionics Engineering Center, now ILA Secretary) 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 co-chairmen of the FDI/FDE Working Group.

Persistent doubts, expressed in that *IONJ* letter, were later vindicated in an independent investigation by P. Nisner and R. 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). Those authors found that 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 in *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.

There is still more. Efforts to obviate the limitations of GO/NO-GO integrity testing also failed to gain committee approval. As one result, consider a test with a maximum allowable number N of missed detections – irrespective of whether each may be a near-miss or a *blunder* – with the following 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. <u>Decision</u> : *Accept*
- RCVR #2 produces $N+1$ missed detections, each occurring with errors exceeding allowable levels only slightly. <u>Decision</u> : *Reject*

That deficiency in acceptance criteria has never been corrected.

Simultaneous appearence of two or more of the various problems previously described would still be unlikely. We can bend over backwards to acknowledge that – but there are no guarantees. The point to be made now 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 interruption, multipath, blockage, sub-mask elevation, superfluous azimuth geometry, •••). 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 independent (e.g., LF) data for consistency checks, with appropriate scaling from error statistics, can enable detections that otherwise could go unnoticed.

The low-cost feature should make retention of Loran capability an easy decision. An opportunity to obtain a small budgetary "saving" would call to mind the overconfidence of

- Amoco before Amoco-Cadiz or
- Exxon before Exxon Valdez – or
- the "best-and-the-brightest" economists, acting with serene confidence, until one nanosecond before the collapse.

This dialogue is necessitated by considerations of safety. A fiasco would not be a welcome event at this time. To anyone contemplating a minor cost saving that deprives the industry of a vital backup, I have three words to say:

Dont do it.

James L. Farrell
VIGIL, Inc.
March 2009