A Critique of Several Failure Detection Approaches for Navigation Systems

THOMAS H. KERR

Abstract—**While the useful structural observations of [1] are laudable for applying "Luenberger observers" in detecting abrupt failures that may occur in deterministic time-invariant linear systems, it is reminded here that these new results are not appropriate to apply to the original navigation and avionics applications that motivated the precursor studies. The original motivating applications were described by stochastic linear systems and used Kalman filters to detect the occurrence of failures. Several barriers are reviewed here that plagued the predecessor investigations (but were previously overlooked) and unfortunately are still not circumvented by the novel approach of [1].**

Status Review and Alleged Soft Spots

The recent investigation of failure detection of linear systems [1] credited two precursor 1971 and 1973 C. S. Draper Laboratory Studies [3], [4], but neglected to mention the fairly recent 1986 followup of [2] along the same lines as [1]. All of these predecessor studies dealt with failure detection in navigation applications described by stochastic time-invariant linear system models with additive Gaussian white process and measurement noises being present, and sought to use Kalman filters tuned in this application context to detect *a priori* specified failures [with occurrences that were previously considered and subsequently anticipated to be likely (cf. [6])]. Since [1] (and [2]) deal exclusively with time-invariant deterministic systems devoid of noise terms, exclusive use of observers suffice for failure detection in this more benign context.

While [1] does make some excellent structural observations for their noise-free case, the caveats offered in [5] explain why the techniques of [1] apparently cannot be conveniently (or otherwise) carried over to the case of noise being present (as encountered in the navigation and avionics applications which, in fact, originally motivated the investigations of [2]–[6]).

For the convenience of the reader, the caveats of [5, sect. 4, p. 97] that pertain to the techniques of [1]–[4] are repeated below. The so-called model following approach, pursued by both R. V. Beard and H. L. Jones in [3] and [4], respectively, requires that the failure detector possess the same mathematical structure as a Kalman filter (i.e., incorporating a system model). However, in [4] the filter gains are chosen by Jones *not* to minimize the mean square error of estimation, as done in an optimal Kalman filter; but are chosen instead to emphasize or enhance the estimates of the failure mode states and to *not* necessarily satisfy any other objectives such as acceptably tracking the other important system states that necessitated the use of a Kalman filter in the first place. Consequently, to be feasible for use, a second Kalman filter would be needed so that one could be used for the usual tracking and estimation functions while the other is used to detect the presence of prespecified or previously characterized failure modes. The approach of these two

Manuscript received March 16, 1988; revised July 28, 1988. This work was supported by the Department of the Air Force.

The author is with M.I.T. Lincoln Laboratory, Lexington, MA 02173.

IEEE Log Number 8927763.

authors also makes use of a novel decomposition[1] of the state space into the controllable (observable) and uncontrollable (unobservable) subspaces. This decomposition is especially amenable to purely deterministic systems subject to failures, but some questions relating to extent of applicability are raised when these same concepts are extended in an attempt to apply them to failure detection in systems having plant and measurement noises (as are frequently encountered in most navigation applications). The random contribution of the effects of noises can defy confinement[2] of the failure response to the controllable (observable) subspace as is otherwise exploited to an advantage in [1]–[4] in the case of failures in a purely deterministic system. Perhaps averaging over a time window of measurements to see whether the result is within epsilon of the subspace before making a failure/no-failure decision will reduce this deleterious effect of being bumped out of the failure mode subspace by the effect of the zero mean random noises that are present.

One particularly important criterion that is frequently overlooked but is especially appropriate as a test against reality for failure detection approaches proposed for (avionics/navigation) applications is further emphasized here now. In general, there is an underlying state variable truth model of fairly high dimension that completely describes the detailed error evolution of the (augmented navigation) system consisting of several components. However, typically only a reduced-order Kalman filter (using just the most significant states) is implemented on-line for real-time applications due to the practical constraints on allowable computational delay to be incurred and computer memory available. Many common failure detection approaches were derived using system descriptions and Kalman filters or Luenberger observers that are of the same dimension as the truth model or full (navigation) error model and the rigor of the derivations underlying the detection method critically depend on the filter residuals being white and unbiased (or the error signal being zero for observers) in the unfailed nominal situation that is typically assumed to be the prevalent mode of operation. In practice, however, the filter residuals can be nonwhite or biased (or the error signal can be nonzero) for the following reasons:

1) because a failure occurred:

2) because a bad measurement was received (i.e., presence of statistical outliers or data gaps):

3) because of the standard use of a reduced-order suboptimal filter or compensator model in the application [11], [12] as is routinely implemented in navigation applications due to constraints on computational capacity available.

Any failure detection approaches that do not explicitly acknowledge the last two reasons above as possibilities consequently incorrectly attribute any nonwhiteness (or nonzero error signal) encountered in the application to be solely due to the occurrence of a failure. The simplistic solution of just raising the decision threshold in order to compensate does reduce false alarms but makes the test less sensitive to actual failures and can cause missed detections when failures do occur.

As mentioned in [5, p. 969, footnote], recall that, in general, the linearization of a nonlinear system is time-varying [7, pp. 53, 54]. In seeking to apply the failure detection techniques of [1]–[4] to linearized nonlinear systems, it should be acknowledged that these techniques have only been developed or posed to date for time-invariant linear system structures. However, there are other approaches to failure detection besides just [13], [14] (as surveyed in [8, sect. II]) that are applicable to time-varying linear systems even with additive Gaussian white noises being present and even constrained to use a reduced-order model of the system [9], [10] (as yet to be addressed in the approaches of [1]–[4]).

In fairness, it should be mentioned that many other alternative approaches to failure detection apparently also suffer from the same weaknesses identified above (as discussed further in [5], [8]).

[1] The analytic methodology provided in [3], [4] and apparently embraced by [1] and [2] for implementing the fundamental decomposition can be invoked only for *time-invariant* linear system models.

[2] A technique to get around this thorny problem has recently been proposed in [15, sect. 3.4, 3.5]. Results using this new approach have yet to be demonstrated in the open literature.

REFERENCES

[1] J. E. White and J. L. Speyer, "Detection filter design: Spectral theory and algorithms," *IEEE Trans. Automat. Contr.*, vol. AC-32, pp. 593–603, July 1987.

[2] M.-A. Massoumnia, "A geometric approach to the synthesis of failure detection filters," *IEEE Trans. Automat. Contr.*, vol. AC-31, pp. 839–846, Sept. 1986.

[3] R. V. Beard, "Failure accommodation in linear systems through self-reorganization," Ph.D. dissertation, MTV-71-1, Dep. Aeronaut. and Astronaut., Mass. Inst. Technol., Cambridge, MA, Feb. 1971.

[4] H. L. Jones, "Failure detection in linear systems," Ph.D. dissertation, Dep. Aeronaut. and Astronaut., M.I.T. C. S. Draper Lab. Rep. T-608, Aug. 1973.

[5] T. H. Kerr, "The controversy over use of SPRT and GLR techniques and other loose-ends in failure detection," in *Proc. Amer. Contr. Conf.*, San Francisco, CA, June 1983.

[6] J. S. H. Liu and H. L. Jones, "Linear manifold constrained GLR," *IEEE Trans. Automat. Contr.*, vol. AC-22, pp. 988–989, Dec. 1977.

[7] R. J. Schwarz and B. Friedland, *Linear Systems.* New York: McGraw-Hill, 1965.

[8] T. H. Kerr, "Decentralized filtering and redundancy management for multisensor navigation," *IEEE Trans. Aerospace Electron. Syst.*, vol. AES-21, pp. 83–119, Jan. 1987; corrections in May and June 1987.

[9] ——, "The proper computation of the matrix pseudoinverse and its impact in MVRO filtering," *IEEE Trans. Aerospace Electron. Syst.*, vol. AES-21, pp. 711–724, Sept. 1985.

[10] ——, "Computational techniques for the matrix pseudoinverse in minimum variance reduced-order (MVRO) filtering and control," in *Control and Dynamic Systems, Vol. 28: Advances in Algorithms and Computational Techniques for Dynamic Systems Control,* Part 1 of 3, C. T. Leondes, Ed. New York: Academic, 1988.

[11] D. D. Boozer and W. L. McDaniel, "On innovation sequence testing of the Kalman filter," *IEEE Trans. Automat. Contr.*, vol. AC-17, 1972.

[12] W. C. Martin and A. R. Stubberud, "An additional requirement for innovations testing in system identification," *IEEE Trans. Automat. Contr.*, vol. AC-19, 1974.

[13] T. H. Kerr, "Real-time failure detection: A nonlinear optimization problem that yields a two-ellipsoid overlap test," *Journal Optimiz. Theory Appl.*, vol. 22, pp. 509–535, Aug. 1977.

[14] ——, "False alarm and correct detection probabilities over a time interval for restricted classes of failure detection algorithms," *IEEE Trans. Inform. Theory.*, vol. IT-20, pp. 619–631, July 1982.

[15] P. S. Min, "Detection of incipient failures in dynamic systems," Ph.D. in the Dep. Elect. Eng. Univ. Michigan, Ann Arbor, 1987.