March 1984 LIDS-R-1306

Laboratory for Information and Decision Systems
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

Final Report on the Development of Methodologies for the Detection of System Failures, for the Design of Fault-Tolerant Control Systems, and for the Analysis of Systems Containing Switches and Subject to Abrupt Changes

ONR Grant No. N00014-77-C-0224

To: Dr. Charles Holland
Mathematics Program (Code 432)
Office of Naval Research
800 North Quincy Boulevard
Arlington, Virginia 22217

SUMMARY

A brief description of the research carried out by faculty, staff, and students of the M.I.T. Laboratory for Information and Decision Systems under ONR Grant No. N00014-77-C-0224 is described. The period covered in this final report is from October 1, 1981 through March 31, 1984. A brief summary of research contributions from October 1, 1981 through April 30, 1982 is contained in the continuation proposal [17] for this Grant.*

The fundamental objective of this project was the development of a firm theoretical foundation and a set of analytical tools for the design of failure detection systems, estimation algorithms for systems subject to abrupt changes, fault-tolerant control systems, and control systems containing switches. In the following sections we overview the research that has been performed in these areas during the indicated time period. We have also included a complete list of the papers and reports that have been written as a result of research performed under this contract.

*This proposal was written for a two-year period, October 1, 1982 through September 30, 1984; funding was approved only for the first year.

I. Development of a Failure Detection Methodology

As summarized in [17], there are three fundamental problems that must be addressed in order to develop a useful and complete failure detection methodology:

(1) The generation of failure-indicating signals; that is, signals which behave in characteristically distinct fashions when specific failures occur

(2) The development of high performance sequential decision rules based on the signals determined in (1)

(3) The analysis of performance of the overall system defined in (1) and (2)

Our efforts in the first of these areas are documented in [6, 12, 15-21] with the last 4 of these having been developed in the period since the appearance of [16]. The two major questions we have attempted to answer are: (i) a unified characterization of redundancy in dynamical systems and of the ways in which this redundancy can be utilized for generating signals for use in failure detection; and (ii) the development of signal generation procedures which take into account model uncertainties in order to produce signals whose characteristics are optimally robust. Question (i) is addressed in [18, 19]. In [18] we provide a linear-algebraic definition of all possible parity relations and discuss the ways in which these relations can be used to generate "parity-check" signals: (a) instantaneous computation of parity checks; (b) open-loop integration of the dynamic relation defined by the parity check; (c) closed-loop filtering based on the dynamic relation. In (b), (c) we view a parity check as a reduced-order (ARMA) model for the temporal variation of a particular component of the output vector. In this model the inputs consist of the inputs to the original system together with the other components of the output. Closed-loop filtering involves designing a Kalman filter with the output consisting of the single component of the original system output whose dynamics are being described. It is straightforward to

generalize this approach to combining several parity relations to produce vector parity-check signals using any of the 3 methods described previously. In [19] we provide a frequency domain characterization of parity checks. This approach has the advantage of allowing one to consider all orders of parity checks at once (where the order of a parity check equals the maximum lag in the output components appearing in the parity relations). Because of this we are able to define a procedure for the construction of a complete set of minimal-order parity checks, where by complete we mean that all other parity relations can be expressed completely in terms of this set.

We have developed two complementary approaches to Question (ii). In [18] we formulate the problem of choosing parity checks which produce the smallest mean-squared value under worst-case parameter values at a specified operating point. This formulation resulted in a complex optimization problem which does, however, allow one to develop adaptive, gain-scheduled parity checks as a function of operating point. In [19-21] we consider an alternative approach which is computationally far simpler and which produces a complete set of parity checks which are ordered in terms of their robustness. The basis for this approach is the geometric interpretation of a parity check as a projection of a time window of output values onto a subspace which, in the case of a perfectly known model, is the orthogonal complement of the subspace of possible output sequences when no failure has occurred. Clearly this orthogonality cannot be assured if there are model uncertainties, but we can attempt to choose a subspace onto which we project which is "as orthogonal as possible" to all possible output sequences under no-fail conditions given a specified range of possible parameter variations. Several formulations of this problem are given in [19-21]. The one which leads to a simple computational procedure is the following. We assume

that we have discretized the set of possible parameter values, so that we can index the possibilities from 1 to N. Let $Z_1,\ldots, Z_N$ denote matrices whose columns form orthonormal bases for the spaces of possible output sequences under each of the possible parameter choices, i.e., Z_i is a basis for the range of

$$\begin{bmatrix} C_i \\ C_iA_i \\ \vdots \\ C_iA_i^p \end{bmatrix} \tag{1}$$

where p is the order of the parity check under consideration. Let G be a matrix whose columns form an orthonormal basis for a candidate space onto which we would project output sequences in order to generate parity checks. If we could obtain perfect performance, each of the matrix products $G'Z_i$ would be identically zero. Consequently, a reasonable performance measure for choosing G would be

$$J^*(k) = \min_{G'G=I_k} \sum_{i=1}^{N} \|G'Z_i\|_F^2 \tag{2}$$

where k denotes the chosen dimension of G, I_k is the k x k identity matrix, and $\|\cdot\|_F$ denotes the Frobenius norm:

$$\|M\|_F^2 = \sum_{i,j} M_{ij}^2 \tag{3}$$

The solution to this problem is the following: Compute the singular value decomposition of the matrix

$$Z = \left[Z_1 \vdots Z_2 \vdots \ldots \vdots Z_N \right] \tag{4}$$

Let the singular values be

$$\sigma_1 \leq \sigma_2 \leq \sigma_3 \leq \cdots \tag{5}$$

and let the corresponding left-singular vectors be g_1, g_2,... . Then

$$G^* = \left[g_1 \vdots \cdots \vdots g_k \right] \tag{6}$$

and

$$J^*(k) = \sum_{i=1}^{k} \sigma_i^2 \tag{7}$$

Thus we see that g_1 represents the best parity check with figure of merit σ_1^2, g_2 is the next best with σ_2^2 as its measure of robustness, etc.

In addition to this basic result we have obtained some extremely important variations and extensions of this result, all of which reduce to the computation of the singular values of a single matrix similar to (4), and each of which overcomes a limitation of the formulation described to this point. These extensions are:

- The incorporation of unequal weights in (2) in order to reflect the relative likelihood of different parameter values
- The consideration of scaling issues. Specifically not all directions in Z_i are equally likely. By assuming that we have a scaling matrix P so that Px is equally likely to be in every direction (P is a square root of the inverse covariance of x), we obtain a modification of (4) which correctly takes scaling into account.
- The inclusion of process and measurement noise. We have shown how to modify (4) not only to take scaling into account but also to take noise into account by adding additional columns representing directions of maximal noise sensitivity.
- The consideration of the robust detection of a particular failure mode by minimizing the sum of the $\|G'Z_i\|_F^2$ for all of the Z_i corresponding to normal operation minus the sum of similar terms for the Z_i corresponding to the particular failure mode. This involves a novel generalization of the motion of singular value decompositions.

We consider the results described above to be significant. In addition, they provide a promising foundation for the consideration of a variety of additional problems. Principal among these is the generation of a set of parity checks which allow not only robust detection but also robust distinguishability of a set of specified failure modes. In addition there are excellent reasons to generalize our notion of parity relation in order to take advantage of known temporal properties of parity relations under normal and failed conditions -- e.g. if model uncertainty may cause a bias in a particular parity check, the parity check might still be good if, for example, a particular failure causes a sinusoidal or ramp-like variation in the value of the parity signal. Using such knowledge leads directly to the idea of interpreting parity relation robustness in the frequency domain using the deterministic results in [19] as a starting point. Other possible directions include the investigation of actuator failure detection and of the relative robustness of the 3 methods for generating parity signals from a parity relation.

The second and third problems -- sequential decision rules and performance analysis for failure detection systems are tightly coupled, as a method for the latter is needed if a recursive optimization algorithm is used to determine the former. In the recent past we have modified and extended the results in [6] in the recently written extended version of [13]. Beyond this, we have initiated a research effort whose aim is to produce a computationally efficient procedure for the accurate evaluation of decision rule performance. Unlike the quadrature methods used in [6, 13] in this effort we attempt to blend together a variety of optimization-based bounding methods (see [17]) for an example) with quadrature and Monte Carlo techniques in order to obtain efficient, accurate, and partially analytic performance results.

II. Fault-Tolerant Control Systems

As discussed in [16, 17] our research in this area has two major thrusts;

- The design of optimal control strategies for fault-prone systems in which the probabilities of occurrence for some or all of the failure modes depend upon the system state and control.
- The design of optimal switching control strategies for fault-prone systems when the fault-state of the system is not observed perfectly but rather must be estimated using a failure detection system.

Most of our effort has been devoted to the first of these problems, and our results are described in [2, 10, 11, 14-17, 23]. References [14] and [23] contain results obtained during the time period covered by this latest report. As a prelude to the investigation of the state- and control-dependent cases, we undertook and completed a thorough investigation of the problem of optimally controlling a linear system whose parameters and quadratic cost matrices are determined by an independent finite-state Markov process which is observed perfectly. While this is a problem that has received a substantial amount of attention in the past, there remained a variety of open questions regarding the asymptotic properties of the optimal closed-loop system (including, for example, the precise conditions for asymptotic stability of the closed-loop system). Obtaining these results turned out to be essential for our investigation of steady-state properties in the more complex case of state- and control-dependent failure probabilities, and our efforts along these lines are documented in [14] and [23].

In previous status reports we described the basic problem under investigation in which the failure probabilities are piecewise-constant functions of x and u. In the scalar case this results in a structure for the optimal control strategy with an inductive flavor. Using dynamic programming one finds that at each point in time the optimal cost-to-go is a piecewise-quadratic

function of the state. Going back one further step in time, one solves a series of constrained LQG problems each corresponding to assuming that the control and new state lie in one of the several possible regions over which failure probabilities are constant and the cost-to-go is quadratic. The number of such problems to be solved grows as one moves back from the terminal time; however it is possible to gain a significant amount of insight into the structure of the optimal controller so that useful qualitative features and steady-state approximations are obtained. In particular, it is relatively easy to show that the number of problems that actually need to be solved at each stage grows linearly with the time-to-go, while the complete set of possible problems grows exponentially. Also, the controller exhibits the phenomenon of hedging -- that is sacrificing some performance in order to reduce the probability of failure. Also, there is the possibility of regions of avoidance, i.e. parts ot the state space into which the controller never drives the state. We now have an explicit characterization of the conditions under which these phenomena occur, and this has provided us with greatly improved understanding of the performance/reliability tradeoff interest in controllers of this type. In addition, we have developed an efficient algorithm for solving for the optimal control law which avoids all extraneous calculations and uses our characterization of when hedging and avoidance occur. Finally, using the structure of this algorithm and our results on the asymptotic properties of optimally controlled systems subject to independent failures, we have been able to quantify the difference in control law and performance between successive linear-quadratic "pieces", and have shown that these differences approach zero under certain conditions. This then allows us to develop a suboptimal algorithm consisting of a fixed number of pieces which approximates the optimal system to within any specified limits.

In addition to the work just described, we have also completed an investigation of the noisy problem in the case when the noises are bounded. Although the piecewise quadratic structure of the solution is lost in certain parts of the state space, many of the qualitative features are retained, and this leads to possible approximations which again can be made quite accurate. In addition, we have also examined the vector case, which is in one sense much more difficult because of the complex shapes of the boundaries between different regions of the state space. Again approximations can be applied which overcome this complexity at the cost of some increase in the number of regions to be considered. All of our results on the problems just described are presented in [14].

Most of our effort in this portion of our research has been developed to the problem area just described. In [17] we describe a novel approach to the second problem area described at the beginning of this section. In particular, we have formulated and have begun to examine a problem in which a system may fail and where the controller class under consideration is constrained to consist of a set of optimal LQG control systems, one corresponding to normal operation and one for each failure mode and onset time, and a decision mechanism for switching from the normal operation control law to one of the other control laws. This is an unusual sequential decision problem, as the usual tradeoffs among detection delay, false alarms, and misclassifications are accounted for indirectly through their impact on overall closed-loop system performance.

III. Estimation and Control Systems Containing Switches

In [16, 17] we outline a variety of problems involving the development of tools for the analysis of systems and design of estimation and control algorithms for systems containing switches or subject to abrupt change. Our work in this area has two complementary aspects. In the first we are interested in designing controllers or estimators which contain switches themselves, while the second deals with the development of near optimum estimation algorithms for systems which may be subject to abrupt changes.

Our early work in the first of these two areas is described in [1, 3, 4, 5, 8] in which we analyzed an adaptive control system which, under appropriate conditions, behaved in a switch-like manner. Our analysis indicated a variety of qualitatively different modes of behavior which we were able to characterize. In our most recent work [22] we have investigated the use of discontinuous feedback laws for regulation and tracking control of a certain class of nonlinear systems. The work in [22] is based on a generalization of the concept of sliding modes in which the state of the closed-loop system is driven toward and slides along the surface along which the control law is discontinuous. By using a time-varying surface we are able to obtain perfect tracking in the noise-free case, and in fact this perfect tracking capability is maintained in the presence of bounded disturbances and parameter variations as long as the size of the discontinuity is chosen appropriately. Specifically, in the worst-case the disturbances and parameter variations will work against the nominal dynamics by trying to drive the state away from the sliding surface. By choosing the discontinuity in the dynamics to be large enough this can be overcome, guaranteeing the stability of the surface. Finally, in order to overcome the inevitable chattering of a discontinuous control system, we develop approxima-

tions to the discontinuous control which allow a tradeoff between tracking accuracy and the frequency of oscillation around the desired state trajectory.

The class of nonlinear systems for which this design methodology is developed consists of those nonlinear systems which do not contain nonlinear zeros, i.e. there are not feedforward paths for the control. The simplest example of a system of this type is

$$\begin{aligned} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= x_3 \\ &\vdots \\ \dot{x}_m &= f(x_1, \ldots, x_m) + u \end{aligned} \tag{8}$$

A slightly more complex one is

$$\begin{aligned} \dot{x}_1 &= x_2 \\ &\vdots \\ \dot{x}_m &= f(x_1, \ldots, x_m, z_1, \ldots, z_m) + u_1 \\ \dot{z}_1 &= z_2 \\ &\vdots \\ \dot{z}_m &= g(x_1, \ldots, x_m, z_1, \ldots, z_m) + u_2 \end{aligned}$$

and from this the general case should be obvious. Consider the system (8) and suppose that we would like $x_1(t)$ to track $\xi(t)$ for $t \geq 0$. We assume that

$$\frac{d^k x}{dt^k}(0) = \frac{d^k \xi}{dt^k}(0) \qquad k = 0, \ldots, m-1 \tag{10}$$

Let $x = (x_1, \ldots, x_m)$, $\rho = (\xi, \dot{\xi}, \ldots, \xi^{(m-1)})$. Then a useful sliding surface is

$$s(x,t) = C' [x(t) - \rho(t)] \tag{11}$$

where $C' = (C_1, \ldots, C_{m-1}, 1)$. Then if we remain on the sliding surface it is not difficult to see that (10) implies $x(t) = \rho(t)$ for all $t \geq 0$. What one then does is design the control law on either side of $s(x,t)$ so that sliding is assured, i.e. so that $\dot{x}(t)$ always points toward the surface if $x(t)$ is off the surface (see [22] for details). Also, in this case the dynamics of the system on the sliding surface are completely specified by $C_1, \ldots, C_{m-1}$ independent of disturbances and parameter variations which would drive the system off the surface, so that these numbers may be chosen to obtain the desired response characteristics to disturbances along the trajectory. Finally the extension to more general systems such as (9) is relatively straightforward.

The other portion of our research, which has received less attention during the recent past, deals with problems in systems which have very different time scales at which variables evolve, so that variations of some variables appear instantaneous. In some of our recent work we have obtained precise results of this type for nonlinear systems with multiple equilibria which are perturbed by small intensity noise. In particular the process essentially looks over long intervals like a linear process near a particular equilibrium and then jumps to another equilibrium. This suggests an estimator structure which is vastly simpler than the full nonlinear estimator for such a system which by its nature looks microscopically at the trajectories between equilibria, even though the time of transit is very short. By sacrificing such fine-structured optimality we believe that we can obtain quantifiably near optimal estimators. We have begun looking at several other problems which have a similar thrust in that one attempts to disregard the fine detail of phenomena evolving at a scale faster than that of interest (see [17]).

PUBLICATIONS

The publications listed below represent papers and reports supported in whole or in part by the Office of Naval Research under Grant N00014-77-C-0224.

1. C.S. Greene, "An Analysis of the Multiple Model Adaptive Control Algorithm," Report ESL-TH-843, Ph.D. Thesis, M.I.T., August 1978.

2. H. Chizeck and A.S. Willsky, "Towards Fault-Tolerant Optimal Control," Proc. IEEE Conf. on Decision and Control, San Diego, Calif., Jan. 1979.

3. C.S. Greene and A.S. Willsky, "Deterministic Stability Analysis of the Multiple Model Adaptive Control Algorithm," Proc. of the 19th IEEE Conf. on Dec. and Cont., Albuquerque, N.M., Dec. 1980; extended version to be submitted to IEEE Trans. Aut. Control.

4. "Status Report Number One, on the Development of a Methodology for the Detection of System Failures and for the Design of Fault-Tolerant Control Systems," Rept. ESL-SR-781, Nov. 15, 1977.

5. "Status Report Number Two, on the Development of a Methodology for the Detection of System Failures and for the Design of Falut-Tolerant Control Systems," Rept. LIDS-SR-873, Dec. 27, 1978.

6. E.Y. Chow, "A Failure Detection System Design Methodology," Ph.D. Thesis, Dept. of Elec. Eng. and Comp. Sci., M.I.T., Nov. 1980.

7. A.S. Willsky, "Failure Detection in Dynamic Systems," paper for AGARD Lecture Series No. 109 on Fault Tolerance Design and Redundancy-Management Techniques," Athens, Rome and London, October 1980.

8. "Status Report Number Three, On the Development of a Methodology for the Detection of System Failures and for the Design of Falut-Tolerant Control Systems," Oct. 25, 1979.

9. H.R. Shomber, "An Extended Analysis of the Multiple Model Adaptive Control Algorithm" S.M. Dissertation, M.I.T., Dept. of Elec. Eng. and Comp. Sci., also L.I.D.S. Rept. LIDS-TH-973, Feb. 1980.

10. D.A. Castanon, H.J. Chizeck, and A.S. Willsky, "Discrete-Time Control of Hybrid Systems," Proc. 1980 JACC, Aug. 1980, San Francisco.

11. H.J. Chizeck and A.S. Willsky, "Jump Linear Quadratic Problems with State-Independent Rates," Rept. No. LIDS-R-1053, M.I.T., Laboratory for Information and Decision Systems, Oct. 1980.

12. E.Y. Chow and A.S. Willsky, "Issues in the Development of a General Design Algorithm for Reliable Failure Detection," Proc. 19th IEEE Conf. on Dec. and Control, Albuquerque, New Mexico, December 1980.

13. E.Y. Chow and A.S. Willsky, "Sequential Decision Rules for Failure Detection," Proc. 1981 JACC, June 1981, Charlottesville, Virginia; extended version submitted to the IEEE Trans. Aerospace and Electronic Systems.

14. H.J. Chizeck, "Fault-Tolerant Optimal Control", Ph.D. Thesis, Dept. of Elec. Eng. and Comp. Sci., M.I.T., July 1982.

15. "Status Report Number Four, On the Development of a Methodology for the Detection of System Failures and for the Design of Falut-Tolerant Control Systems," Oct. 1980.

16. "Status Report Number Five, On the Development of a Methodology for the Detection of System Failures and for the Design of Fault-Tolerant Control Systems," Oct. 1981.

17. "A proposal for Extension of Research Under ONR Grant N00014-77-C-0224," May 15, 1982.

18. E.Y. Chow and A.S. Willsky, "Analytical Redundancy and the Design of Robust Failure Detection Systems," accepted for publication in IEEE Trans. on Automatic Control.

19. X.-C. Lou, "A System Failure Detection Method: The Failure Projection Method," S.M. Thesis M.I.T. Dept. of Elec. Eng. and Comp. Sci., also Rept. LIDS-TH-1203, M.I.T. Lab. for Inf. and Dec. Sys., June 1982.

20. X.-C. Lou, A.S. Willsky, and G.C. Verghese, "Failure Detection with Uncertain Models," invited paper at the 1983 American Control Conference, San Francisco, Calif., June 1983.

21. X.-C. Lou, A.S. Willsky, and G.C. Verghese, "Optimally Robust Redundancy Relations for Failure Detection in Uncertain Systems," submitted to Automatica; also Rept. LIDS-P-1297, M.I.T. Lab. for Inf. and Dec. Sys., April 1983.

22. J.J. Slotine and S.S. Sastry, "Tracking Control of Non-linear Systems Using Sliding Surfaces with Application to Robot Manipulators," to appear in the International Journal on Control.

23. H.J. Chizeck, A.S. Willsky, and D.A. Castonon, "Markovian Jump Linear Quadratic Optimal Control in Discrete Time," Proc. 22nd IEEE Conf. on Dec. and Control, San Antonio, Texas, Dec. 1983.