Proceedings of the 11th
KACC, October 1996

AN OVERVIEW OF DECENTRALIZED OPTIMAL FAULT-TOLERANT SUPERVISORY CONTROL SYSTEMS [1]

°K.-H. Cho * and J.-T. Lim * [2]

* Department of Electrical Engineering, Korea Advanced Institute of Science and Technology
373-1 Kusong-dong, Yusong-gu, Taejon, Korea
Tel : +82-42-869-5441 Fax : +82-42-869-3410 E-mail : jtlim@stcon.kaist.ac.kr

Abstracts In this paper, we discuss decentralized optimal fault tolerant supervisory control issues on the basis of failure analysis and diagnosis from the angle of discrete event dynamic system. We address the detectability and the observability problems, and develope fault tolerant supervisory control system upon the failure analysis and diagnosis schemes. A complete min-cut is introduced and the procedure for finding the achievable or nonachievable layered optimal legal sublanguages is suggested for a preferential option among the reachable states in the controlled plant. A layered optimal supervisory control framework is proposed upon these. We extend the concept of decentralized supervisory control by considering the problem of combination of decentralized with centralized control in case pure decentralized control happens to be inadequate. We introduce the concept of locally controllable pair and present a hybrid decentralized supervisory control framework. Finally, we propose the analytical framework for a decentralized optimal fault tolerant supervisory control systems.

Keywords Discrete event dynamic system, Supervisory control, Fault tolerant system, Layered optimal control, Hybrid decentralized control

1. Introduction

Since the demands on reliability and safety of modern complicated systems are increasing, the analytical and numerical work on failure diagnosis is in progress today and many techniques have been developed [1]-[2]. Recently, this problem has also been studied in the framework of discrete event dynamical systems (DEDSs) [3]. In the literature [4], the unexpected changes in the system, such as component faults and variations in operating conditions, are classified qualitatively. A "fault" is understood as an unexpected change in the system that tends to degrade the overall system performance, although it may not represent the "failure" of physical components. The term fault rather than failure is used to denote a malfunction rather than a catastrophe. The term failure suggests a complete breakdown of a system component or function, whereas the term fault may be used to indicate that a malfunction is present but it may be tolerable. However there exists no clear and quantitative classification at this time. We propose a DEDS approach to the failure analysis and diagnosis problem. Based on it, we adopt the framework proposed by Ramadge and Wonham [5], [6] for the study of fault tolerant supervisory control systems. The overall model is thus a state model of the open loop system dynamics with external control. See [5], [14] for a synopsis of the framework and some of the principal results.

For a given DEDS, we do a failure analysis to classify faults and failures, and to find tolerable fault event sequences (TFESs), then design a supervisor upon the TFESs and construct a failure diagnosis scheme. Once the fault tolerant supervisory control system (FTSCS) is constructed, the behavior of the system withn the reachable state space of FTSCS can be further optimized through layered optimal supervisory control. The complexity problem occurring during the design of supervisor can be solved essentially by the hybrid decentralized supervisory control scheme. Finally, we propose an analytical framework for decentralized optimal fault tolerant supervisory control systems (DOFTSCSs) including all of the aforementioned issues.

2. Fault Tolerant Supervisory Control

The detectability problem for state identification and the observability problem for achievable legal languages are studied for DEDSs. Especially we propose more specific and partitioned conditions — C-observability and D-observability conditions — to check the observability of the given legal language. Then a systematic way for analyzing DEDSs is proposed to classify faults and failures quantitatively and to find tolerable fault event sequences embedded in the system. An automated failure diagnosis scheme with respect to (w.r.t.) the nominal normal operating event sequences

[1]This work was supported by the Korean Science and Engineering Foundation.

[2]To whom all correspondence should be addressed.

(NNOESs) and the supervisory control for achievable tolerable fault event sequences are presented. In addition, the supervisor failure diagnosis w.r.t. the tolerable fault event sequences is addressed. We present an analytical framework for FTSCSs as follows.

First, for a given DEDS G do failure analysis by off-line to classify faults and failures, and to find any TFES embedded in the system if it exists. Once we found TFESs, let them be a legal language K, then check C or D-observability conditions to determine whether it is achievable or not. If it is not achievable then reconstruct an achievable legal language K', e.g., by computing the supremal normal sublanguage [13] from the TFESs. If there is no achievable TFES then let NNOESs be a legal language K. Next, design a supervisor $\mathcal{S}$ along the legal language K. During the operation, the control system monitors the supervised behavior of G. If a failure is detected, then the control system starts failure diagnosis to find the source failure and change the status of G into repairing mode. If a fault is detected, then the control system automatically reconfigures for the other TFES within K. The control system starts supervisor failure diagnosis for a normal event if it does not lie on the scheduled TFES and change the status of $\mathcal{S}$ into repairing mode. The overall structure of the proposed FTSCS is shown in Fig. 1.

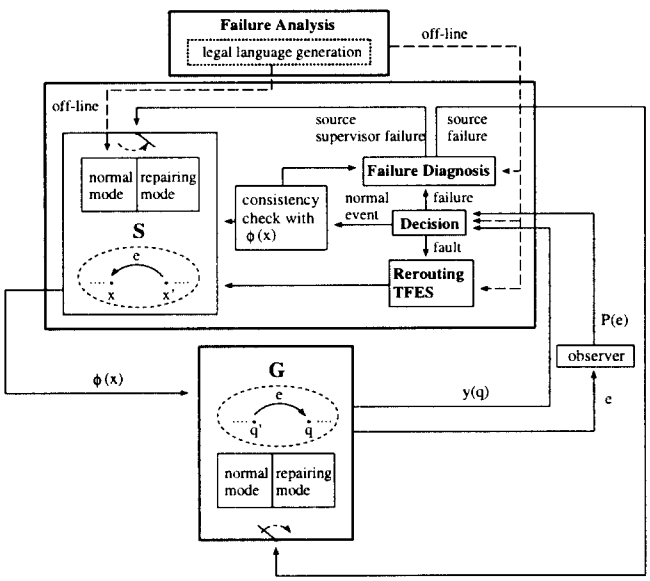

Fig. 1: Overall structure of FTSCS with partial observations.

3. Layered Optimal Supervisory Control

We consider an optimal supervisory control problem to optimize the behavior of the proposed FTSCSs. The concept of optimal supervisory control of DEDSs has been established on the framework proposed by Ramadge and Wonham [5]; a DEDS, also called plant, has been modeled as a finite state machine (FSM) and is controlled by disabling some of its transitions. In the literature [7]–[8], two types of cost functions were defined generally: a cost of control function corresponding to disabling transitions in the FSM, and a penalty of control function corresponding to reaching some undesirable states or not reaching some desirable states in the controlled system. The optimal supervisory control problem was defined to determine for each transitions in a FSM whether to disable or enable it, so that the net cost is minimized. It was shown in [8] that this problem is equivalent to determining an optimal partition of the state space, Q of the FSM, G into the set of states that remain reachable in the controlled plant and the set of remaining unreachable states. Moreover the desirable optimal partition was determined using the max-flow min-cut theorem [9], a technique for optimal partitioning of directed graphs. In this way, we could determine an optimal state-feedback supervisor resulting the subgraph of the plant graph so that the net cost of disabling transitions, that of reaching undesirable states, and that of not reaching desirable states is minimized. The synopsis of the framework and some of the existing main results are shown in [8]. However, the concept of a specified marked languages and the preferential option among the reachable states in the controlled plant in view of certain performance measure can not be encompassed in this framework. Thus we propose a unified framework, layered optimal supervisory control system (LOSCS), to obtain the achievable optimal legal language and to further classify the reachable states according to the performance measure resulting achievable or nonachievable layered optimal legal sublanguages. All of the achievable or nonachievable optimal or suboptimal legal languages and the intractable state information for nonachievable sublanguage case should be computed by off-line and stored in a data base system. During the control, the supervisor is reconfigured according to the optimal legal language in each varying situation by accessing the data base. The analytical framework for the LOSCSs is shown schematically in Fig. 2.

4. Hybrid Decentralized Supervisory Control

To complement the proposed analytical frameworks from the standpoint of computational complexity and flexibility, we consider a decentrlized supervisory control problem. The earlier works of supervisory control were extended to formulate a decentralized approach to supervisor synthesis [10]–[11]. In this approach the control task is split into several subtasks, these are solved using the existing theory, and the resultant "subcontrollers" are combined to form a solution to the original problem. Such a construction is referred to as a *decentralized synthesis*, and the resultant controller

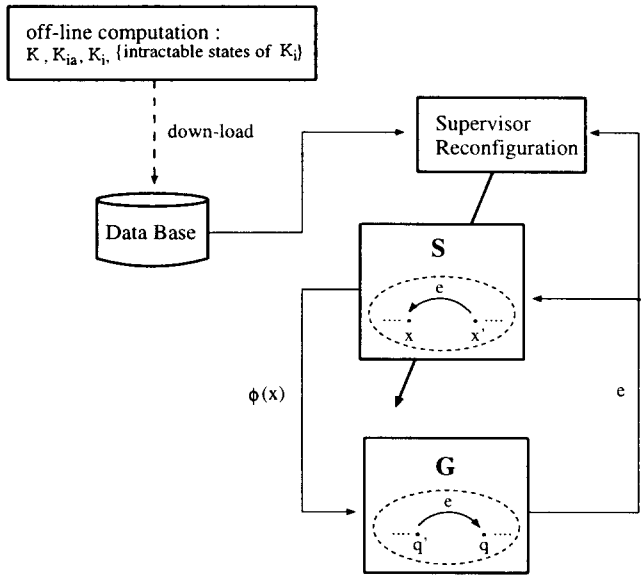

Fig. 2: Framework for LOSCS.

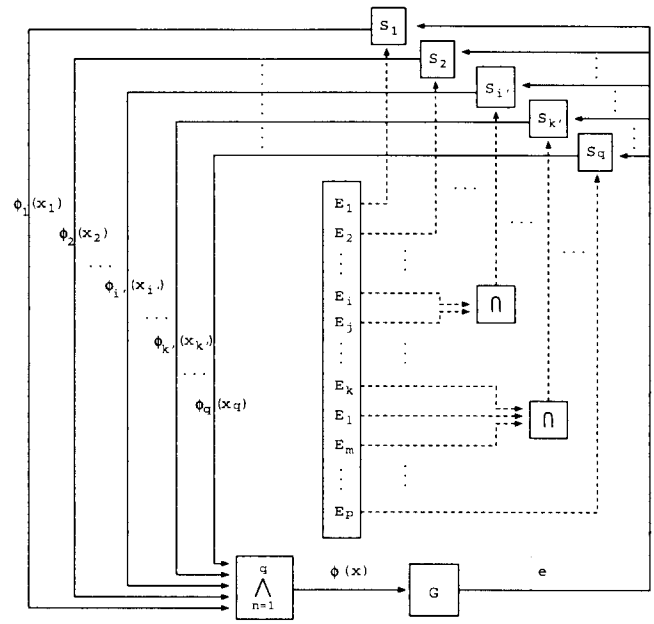

Fig. 3: Framework for hybrid decentralized supervisory control systems.

as a *decentralized supervisor*. The decentralized synthesis has two advantages: complex problems can be decomposed into simpler units and the resultant controller has greater flexibility, i.e., it can be more easily modified, updated, and maintained. However there still remains two important problems to this approach: detailed conditions to ensure that the resultant decentralized supervisor is nonblocking, and establishing an optimal — the term "optimal" in this case will mean supremal in the sense of subset inclusion — combination of decentralized with centralized control in case pure decentralized control happens to be inadequate. In the current framework little could be said about the former problem aside from the test for nonconflicting languages [12]. Recently a new approach is explored by employing priority functions instead of conjunction operators for combining subcontrollers [11]. For the latter problem, nothing could be said at present time. We explore this problem and suggest an analytical framework for hybrid decentralized supervisory control systems (HDSCSs). For a given overall legal specification expressed in terms of local specification, we can find the optimal combination of decentralized with centralized control even though G is not locally controllable. These constitute the analytical framework for HDSCSs, which is shown schematically in Fig. 3.

5. Decentralized Optimal Fault Tolerant Supervisory Control Systems

Consider a DEDS G which is obtained by composing its component DEDSs or which can be naturally split into those components. Assume also that the global specification (control objective) is given by its component parts. The global or local specifications are further assumed to be sublanguages of each marked language without loss of generality.

We can obtain locally controllable pairs (LCPs) including locally controllable ones for the given local specifications within the HDSCS framework if possible. Once we find all of the LCPs then this implies that the concurrent action of supervisors, obtained by extending the local fault tolerant supervisors based upon the TFESs of combined parts (or part) corresponding to each LCP (or locally controllable one, respectively), will ensure the global behavior of G along its TFESs. This follows from the fact that the supremal controllable sublanguages are sublanguages of the set of all possible TFESs and from the main results of the HDSCS in Section 4.. Thus we can make the global system modularized, and can do the failure analysis and diagnosis for each module to obtain fault tolerant subsystems and diagnosis schemes within the FTSCS framework. Namely, we classify the faults and failures, and find the embedded TFESs, to obtain the (supervisor) failure diagnosis schemes and fault tolerant supervisory control systems for each module corresponding to LCPs or locally controllable ones, from the FTSCS in Section 2.. Moreover we can optimize the behavior of each fault tolerant subsystem w.r.t. a certain performance measure which consists of cost functions and penalty functions on the LOSCS framework in Section 3.. Although, in this case, the HDSCS does not generate the optimal behavior of the overall system in the sense of subset inclusion, it still ensures the fault tolerant behavior of the overall system. These apply also to the case when we can not find LCP for a certain local specification even though it is controllable in the local sense.

If any of the local specifications is not controllable then this implies that there is no TFES for the corre-

sponding component subsystem. Hence the best way we can do in this case is to operate this subsystem on a NNOES derived from failure analysis or nonachievable layered optimal legal sublanguage within LOSCS framework. For the other part of local specifications, we can construct a (optimal) FTSCS in a decentralized way, as before. If a failure is detected during the operation, we can identify its source failure for the subsystem through the failure diagnosis scheme.

The aforementioned strategy with the analytical framework of FTSCS in Section 2., LOSCS in Section 3., and HDSCS in Section 4. serves to construct the analytical framework of DOFTSCSs.

6. Conclusions

In this paper, a DEDS approach has been utilized to propose an analytical framework for supervision and monitoring of modern man-made systems. We have discussed failure analysis and diagnosis, fault tolerant supervisory control with partial observations, layered optimal supervisory control, and hybrid decentralized supervisory control issues related to large complex systems from the point of view of DEDS. Finally, we have proposed the analytical framework for DOFTSCSs combining the aforementioned issues.

References

[1] S. Lapp and G. Powers, "Computer aided synthesis of fault trees", *IEEE Trans. on Reliability*, vol. 26, pp. 2–13, 1977.

[2] D. A. Handelman and R. F. Stengel, "Combining expert system and analytical redundancy concept for fault-tolerant flight control", *J. of Guidance, Control, and Dynamics*, vol. 12, pp. 39–45, 1989.

[3] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis, "Failure diagnosis using discrete event models", in *Proc. IEEE Conf. on Decision and Control*, Lake Buena Vista, FL, 1994, pp. 3110–3116.

[4] R. J. Patton and J. Chen, "Review of parity space approaches to fault diagnosis for aerospace systems", *J. of Guidance, Control, and Dynamics*, vol. 17, pp. 278–285, 1994.

[5] P. J. Ramadge and W. M. Wonham, "Supervisory control of a class of discrete event processes", *SIAM J. of Control and Optimization*, vol. 25, pp. 206–230, 1987.

[6] P. J. Ramadge and W. M. Wonham, "The control of discrete event systems", *Proc. IEEE, Special Issue on Discrete Event Dynamic Systems*, vol. 77, pp. 81–98, 1989.

[7] K. M. Passino and P. J. Antsaklis, "On the optimal control of discrete event systems", in *Proc. IEEE Conf. on Decision and Control*, Tampa, FL, 1989, pp. 2713–2718.

[8] R. Kumar and V. K. Garg, "Optimal supervisory control of discrete event dynamical systems", *SIAM J. Control and Optimization*, vol. 33, pp. 419–439, 1995.

[9] T. C. Hu, *Combinatorial Algorithms*, Addison-Wesley, Menlo Park, CA, 1982.

[10] P. J. Ramadge and W. M. Wonham, "Modular feedback logic for discrete event systems", *SIAM J. of Control and Optimization*, vol. 25, pp. 1202–1218, 1987.

[11] Y.-L. Chen and S. Lafortune, "Modular supervisory control with priorities for discrete event systems", in *Proc. IEEE Conf. on Decision and Control*, New Orleans, LA, 1995, pp. 409–415.

[12] W. M. Wonham and P. J. Ramadge, "Modular supervisory control of discrete-event systems", *Math. of Control, Signals, and Systems*, vol. 1, pp. 13–30, 1988.

[13] R. D. Brandt, V. K. Garg, R. Kumar, F. Lin, S. I. Marcus, and W. M. Wonham, "Formulas for calculating supremal controllable and normal sublanguages", *Systems Control Lett.*, vol. 15, pp. 111–117, 1990.

[14] K.-H. Cho and J.-T. Lim, "Failure diagnosis and fault tolerant supervisory control system", *IEICE Trans. on Information and Systems*, Vol. E79-D, No. 9, pp. 232–240, 1996.