1971

Security of an industrial system.

Sollberger, Melvin Hugh.

Case Western Reserve University

SECURITY OF AN INDUSTRIAL SYSTEM

by

Melvin Hugh Sollberger

SECURITY OF AN INDUSTRIAL SYSTEM

by

MELVIN HUGH SOLLBERGER

Submitted in partial fulfillment of the requirements

for the Degree of Doctor of Philosophy

Thesis Advisor: Dr. James D. Schoeffler

Division of Systems Engineering

CASE WESTERN RESERVE UNIVERSITY

January, 1971

SECURITY OF AN INDUSTRIAL SYSTEM

Abstract

by

MELVIN HUGH SOLLBERGER

The control of security for an industrial system demands an understanding of the causes and effects of disruptive structural disturbances, called contingencies. To reduce the effect of these disturbances one can implement contingency control, contingency prevention and contingency planning. Implementation requires the definition and classification of system constraints. Once classified as either an operating constraint or a load constraint, security with respect to a given contingency can be determined. Based on these constraints, the modes of operation are partitioned into sets which are indicative of the security control actions required prior to, during and after a system emergency. Of particular interest are the actions required prior to a system emergency, because here it is possible to exercise contingency control, that is, to alter the security of the system to make it less susceptible to certain contingencies. Contingency control has been formulated as a constrained optimization problem in which the imposition (relaxation) of security constraints increases (decreases) the security of the system. Security control is universally applicable to all industrial systems. Yet the degree of

implementation depends upon the flexibility of the system and desirability (based upon the trade-off between performance and security).

ACKNOWLEDGEMENTS

The author wishes to give special acknowledgement to his thesis advisor, Professor James D. Schoeffler. Dr. Schoeffler was a constant source of ideas, inspiration and advice. In addition, Doctors Lefkowitz, Mitter, Lasdon, Macko, and Rothenberg were consulted. Their assistance deserves acknowledgement.

The author received a considerable amount of techanical assistance from Mr. Frank E. Murphy, Jr. of the Corning Glass Works, Corning, New York. Without this assistance, the application of security control to a realistic industrial system might not have been realized.

During this study, the author received financial support directly from the United States Navy and indirectly from the industrial sponsors of the Control of Complex Systems Group of the Systems Research Center.

Moral support and constant encouragement were received from the author's wife Dot.

TABLE OF CONTENTS

	Page
Abstract	ii
ACKNOWLEDGEMENTS	iv
TABLE OF CONTENTS	v
LIST OF FIGURES	vi
CHAPTER I	
INTRODUCTION	1
CHAPTER II	
THE CONCEPT OF SECURITY CONTROL	5
CHAPTER III	
THE COST OF SECURITY CONTROL	27
CHAPTER IV	
EXAMPLES OF SECURITY CONTROL	34
CHAPTER V	
EXAMPLES OF CONTINGENCY CONTROL	55
CHAPTER VI	
IMPLEMENTATION, A DETAILED EXAMPLE	76
CHAPTER VII	
SUMMARY AND EXTENSIONS	103
LIST OF REFERENCES	108

LIST OF FIGURES

Figure

2-1 The partitioning of the operating space into modes of operation.

2-2 The partitioning of the normal operating space into secure and insecure regions.

4-1 A block diagram of the glass manufacturing process.

5-1. A subsystem representation of an electrical power system.

5-2 An isolated subsystem of an electrical power system.

5-3 A system representation of the downcomer.

6-1 The I-th subsystem of the downcomer.

6-2 A block diagram of the linear approximation of the I-th section of the downcomer.

6-3 A block diagram of the traditional control system.

6-4 A block diagram of the downcomer contingency control.

6-5 The operating space for the first section of the downcomer.

7-1 A multi-strata control system.

CHAPTER I

INTRODUCTION

Historically, system security has always been a major concern of design engineers, system operators, and management personnel. Yet this concern has not resulted in a comprehensive understanding of system security. The emphasis in the past has been directed in many areas, such as: understanding and designing reliable systems, providing alternatives and system redundancies to allow compensation for certain disruptive disturbances, designing interlocks and prevention systems to prevent the occurance of certain catastrophic events, designing automatic protection devices to place the system in a safe condition after certain events occur, and training operators to evaluate and take action based upon the security (or insecurity) of the system.

The research and literature on reliability is extensive and will not be reviewed in this dissertation. It concentrates on the calculation and/or estimation of reliability of the overall system based upon the reliability of individual components. It is more concerned with the probability of system failure, the measurement of individual reliability, and the mean time between failures than the secure operation of the system.

Whether the system is reliable or unreliable, it will be

subjected to some disturbances which will threaten the structure of the system. These disturbances are not subject to normal compensation. However, by providing alternatives and redundancies the system will be more flexible; and with this flexibility, a well-trained operator can use his knowledge of the system to operate it in a safe, reliable and secure manner. However, different operators may operate the system differently, resulting in differing degrees of safety or security, and consequently different levels of performance. This means that both performance and security are variable and may depend solely upon operator ability. This becomes less acceptable as the systems become more complex and the rate of operator turnover increases.

To insure that certain catastrophic events can not occur or more often will not reoccur, certain designers specialize in preventing events by providing system interlocks. Some events can not be prevented with any degree of certainty and thus it is imperative to protect the system from damage when these events occur. The design of automatic protection devices is concerned with this problem. All of these design efforts are related and more important, they are related to the secure operation of the system.

Recently at Case Western Reserve University, Tomas E. Dy-Liacco (12) took a new and different approach to system security. Using pattern recognition, a computer was programmed to assist the

operator in determining whether or not an electrical power system was secure or insecure. Dy-Liacco's work implied the existance of concepts governing security control, which could be applied to other complex systems.

The purpose of this dissertation is to develop a consolidated and coherent set of concepts for system security. These concepts must be the framework which relates the design efforts to secure operation of a system. More important is the development of concepts which will guide the design of future control systems, capable of controlling the security of a system. These automated control systems must be capable of operating a complex system with the efficiency and the safety of the most experienced and best trained operator, yet with the repeatability of a digital computer. In order to design such a system, one must understand not only security but also the trade-off between security and system performance.

The thesis has been separated into four sections, philosophy, examples, implementation and extensions. Chapters two and three provide the definitions, concepts and philosophy of security control. Then, chapters four and five present some general examples, illustrating the applicability of these concepts. Chapter six is concerned with an actual implementation of contingency control to a complex process. Chapter seven presents

extensions and conclusions caused by (a) the application of security control and (b) the philosophical and conceptual development.

CHAPTER II

THE CONCEPT OF SECURITY CONTROL

In this chapter the concepts of security control will be presented. This will include definitions and explanations of terms to be used in succeeding chapters, such as security, contingencies, constraints, modes of operation, and types of security control.

Contingencies

A contingency is a possible but not certain event or disturbance which is capable of changing the structure of a system; i.e., a disruptive structural disturbance. Since this disturbance or event is uncertain, there is a probability of occurance associated with each contingency, and this probability will vary under differing conditions.

One can consider contingencies to belong to one of two classes: environmentally dependent and environmentally independent contingencies. An environmentally dependent contingency requires a given environment before it is feasible. Without this environment or the satisfaction of a given set of conditions, it is impossible for this contingency to occur. There may be more than one environment in which it can occur and the probability of occurance may vary from one environment to another. Other contingencies are environmentally independent, that is their probability of occurance is independent of the environment. In addition to requiring some environmental

conditions, most contingencies are not isolated events but on the contrary belong to a sequence of events and will not occur unless the preceeding events have already occurred. Even if the environmental and the sequential conditions are satisfied, many contingencies still will not happen without initiation. The initiating action may be a very small disturbance. These three types of conditions can all be collected and expressed as a set of necessary conditions for the occurance of a contingency. The necessary conditions for an environmentally independent contingency are limited to the sequential and initiating conditions.

A contingency can either occur very rapidly or occur over a period of time. If it occurs over a period of time, then it may be possible to terminate the contingency before it disrupts the system's structure.

In order to fully understand contingencies one must consider what constitutes a disruption of the system's structure. If a system is composed of interconnected subsystems and some of the subsystems have more than one mode of operation, then the internal structure of the system can be altered by varying the modes of operation of the subsystems. In some processes the modes of operation may be simply operating within specifications or out of specification. In the simplest of cases each subsystem can be either operative or inoperative. In this case any disturbance which can cause a subsystem failure will change the mode of the

subsystem from operative to inoperative and consequently change the internal structure of the overall system. In this case the contingencies would be the disturbances that can cause a subsystem to fail. In the more general case, in order to enumerate the contingencies, one must list the identifiable subsystems and all the modes of operation for each of these subsystems. There are various failures which can occur in a subsystem and thus change the mode of operation. The disturbances which cause these failures (total or partial) are the contingencies which can be considered for not only this subsystem but also for the overall system. The causes of the contingencies and the subsystem failure are one and the same.

A fact of particular interest is that there are similar disturbances of lesser magnitude that do not result in a structural change, and there may be more than one contingency that results in the same structural change. If there are several contingencies that result in the same structural change and these disturbances differ only in degree or magnitude, then one need only consider the disturbance having the least magnitude rather than the entire family of contingencies. This representative contingency is a critical or threshold disturbance.

In order to appreciate the effect of contingencies on a system, let me consider a system S composed of interconnected subsystems. Some of the subsystems have more than one mode of operation. Thus, the internal structure of the system S can be varied by altering the

modes of operation of the subsystems. One result of this variable structure is the input/out relations will vary with these changes in structure, causing S to appear as a time-varying system.

The system S will not be functional. However, if one identifies the internal structure (topology) then one would expect to find a functional representation associated with each topology. In the case of a static system, let the functional representation of this static system be a vector function. Let the input vector be u (subscripted to denote different input vectors). Let the various internal structures (topologies) of the system S be denoted by T (subscripted to denote different topologies). Let the output vector be y (subscripted to denote different output vectors). For a topology $\underline{T}_j$, and an input $\underline{u}_i$, the output is $\underline{y}_{ij}$.

$$\underline{y}_{ij} = \underline{f}\,(\underline{u}_i\ ,\ \underline{T}_j\ )$$

This indicates that for the same input but different topologies, the output may differ. The system need not be static, however for simplicity this static system will illustrate the pertinent concepts.

Constraints

One of the problems which arises is: after the internal structure has been altered the system may no longer be able to satisfy the demands that are levied on the system. These demands can be expressed as restrictions or constraints that must be satisfied.

Definition: A "constraint" is a restriction on the system variables. For simplicity assume that the constraint does not depend on the topology, then it can be expressed as:

$$\underline{g}\ (\underline{u}_i\ ,\ \underline{y}_{ij}\ ) \leq 0$$

The constraints on a system can have many origins, such as safety, quality control, security, performance, operational and continuity requirements. However for the moment, consider the following two types of constraints:

Definition: A "load constraint" is a constraint that results from performance requirements, such as the supply must equal demand; the supply must be greater than the demand; the demand (order) must be satisfied (filled) within a certain time interval; or the output must meet certain specifications.

Failure to satisfy a load constraint does not jeopardize the system in any way, but results in customer dissatisfaction because the customer's demands (load) are not satisfied. Failure to satisfy a load constraint jeopardizes the goal of the system.

Definition: An "operating constraint" is a constraint that results from an operational requirement, such as a system or component must be operated safely and/or continuously.

Now if all the system constraints can either be classified as an operating or a load constraint, then the system and its constraints can be represented by:

$$\underline{y}_{ij} = \underline{f}\ (\underline{u}_i\ ,\ \underline{T}_j\ )$$

$$\underline{g}\ (\underline{u}_i\ ,\ \underline{y}_{ij}\ ) \leq\ 0$$

where g is a vector composed of the load and operating constraints.

A Normal System

Definition: A system is "normal" if both the operating and load constraints are satisfied.

Let T_1 be one of the normal configurations for this system, that is

$$\underline{y}_{i1} = \underline{f}\ (\underline{u}_i\ ,\ \underline{T}_1\ )$$

$$g\ (\underline{u}_i\ ,\ \underline{y}_{i1}\ ) \leq\ 0$$

are satisfied. If a contingency that causes the topology to change to T_2 occurs, will the system still be normal? The system will be normal if and only if

$$\underline{g}\ (\underline{u}_i\ ,\ \underline{y}_{i2}\ ) \leq\ 0$$

is satisfied. When a contingency occurs and the new topology results in an input/output relation that continues to satisfy the operating and load constraints then the system was secure.

Security

Definition: A system is "secure" with respect to a given contingency if the system is normal before and after the contingency has occured.

Security need not be limited to a single contingency. On the contrary, a system can be said to be secure with respect to a set of contingencies if it is secure with respect to each contingency

of that set. It is assumed that only one contingency of this set occurs during a given period of time; i.e., that period of time under consideration. The set of contingencies with respect to which the system must be individually secure is called "the set of next contingencies". For the purposes of security, each contingency of "the set of next contingencies" is deemed to be imminent. Before considering more than one contingency, consider the case in which the "set of next contingencies" consists of a single contingency. In this case, consider the previous system equations and the load and operating constraints:

$$\underline{y}_{ij} = \underline{f} (\underline{u}_i , \underline{T}_j)$$

$$\underline{g} (\underline{u}_i , \underline{y}_{ij}) \leq 0$$

If one of the normal modes of operation has a topology, T_1 , and the "set of next contingencies" consists of the contingency which causes the topology to change to T_2 , then in order to be secure with respect to this contingency the system must satisfy the following:

$$\underline{y}_{i1} = \underline{f} (\underline{u}_i , \underline{T}_1)$$

$$\underline{y}_{i2} = \underline{f} (\underline{u}_i , \underline{T}_2)$$

$$\underline{g} (\underline{u}_i , \underline{y}_{i1}) \leq 0$$

$$\underline{g} (\underline{u}_i , \underline{y}_{i2}) \leq 0$$

The first two equations will be satisfied because they follow directly from the set of system equations. The first inequality will be

satisfied because T_1 is a topology corresponding to a normal system. The second inequality is a security constraint. By restricting the system to those inputs and outputs which satisfy this inequality, one can insure it will not be violated. This will insure that the system will remain normal even if this contingency occurs. Note that only for this restricted set of inputs and outputs, T_2 is a topology corresponding to a normal system. The unrestricted set of inputs and outputs for this topology may not satisfy this constraint.

Definition: A "security constraint" is a constraint that results from security requirements, i.e., the desire to be secure with respect to a given contingency.

It may be necessary to impose additional constraints on a system, in order to insure that the system is secure with respect to a given contingency. If security were the only consideration, then one might try to select operating and load constraints that were at least as restrictive or more restrictive than the security constraints that are required by the "set of next contingencies". This set of constraints might result in an empty operating space; i.e., the only feasible operating condition is not operating at all. Even if the operating space is not empty, the system performance might be unacceptable when all of the security constraints are imposed. This introduces the very important concept of a trade-off between security and performance. By relaxing the security constraints, improved performance may be realized. By imposing security constraints, the

security is enhanced and the performance may suffer a degradation.

How can one handle the selection of which constraints are to be relaxed and which constraints are to be imposed? As before, there is a set of next contingencies with respect to which the system must be secure. Thus the set of all possible contingencies can be divided into three subsets: those for which the system is always insecure, those for which the system is marginally secure (sometimes secure and sometimes insecure), and those for which the system is always secure.

Alternatives

After the system has been designed with redundant subsystems and other improvements for the sake of reliability, can any more be done? Certainly, a lot more can be done in order to operate this system in a safe and continuous manner. For each contingency there are operating alternatives that can be classified according to whether the action to be taken occurs before, immediately prior to, during or after the contingency occurs.

Without naming these actions, let us consider their nature. The actions taken before a contingency are either to prevent the contingency from occuring or to negate (reduce) the damage if the contingency occurs. Once the contingency begins to occur, prevention is out of the question. However both the minimization of damage or penalties due to the contingency and the prevention of other contingencies are still very important. This can be done by placing the system in a safe mode of operation and restoring the

system to a normal mode of operation as soon as possible. After the contingency has occurred the objectives are similar to the objectives of importance during the contingency, namely insuring the system is safe or secure with respect to other next contingencies and restoring the system to normal as soon as possible. The prevention of contingencies is quite naturally called "contingency prevention". The imposition and relaxation of security constraints to enhance security and thus directly influence the effects of the contingency is called "contingency control". The preparation of action to be taken as soon as the contingency occurs and during the restoration phase is called "contingency planning", and these actions are known as contingency plans until they are executed.

Contingency Prevention

For each contingency the prevention will be different, however the method of contingency prevention is similar. Since there are usually necessary conditions that must be satisfied before the contingency can occur, prevention is directed towards controlling these necessary conditions. This may entail control of either the environmental conditions, the sequential conditions, the initiating conditions or all three.

If a contingency has no necessary conditions, it can not be prevented with any degree of certainty. This is apparent because the absence of necessary conditions implies that 1) the probability of occurance does not depend on the environment; i.e., it

is an environmentally independent contingency, 2) this contingency does not belong to a sequence of events, and 3) an initiating action or condition is not necessary. Based on these facts, this type of contingency is a truly random event that can not be detected or predicted until after it has begun to occur. If this contingency occurs over a period of time, then it may be possible to terminate the contingency before it disrupts the system's structure; i.e., contingency control If it occurs in a very short period of time, then it may be possible to reduce the degree of disruption, by implementing a contingency plan.

Consider a contingency that is not really random, one with necessary conditions. The contingency can be prevented by preventing one or more of the necessary conditions. For example, if sequential conditions exist, that is the contingency belongs to a sequence of events, then by preventing a preceeding event, the sequence can be stopped before the contingency occurs. Often the expected probability of occurance increases as the sequential events transpire. When this is the case, the preceeding events can be used as a forewarning and they can initiate contingency prevention and/or contingency control. If the contingency is environmentally dependent, then efforts to control the environment will result in either partial or total contingency prevention. Total prevention occurs when the contingency becomes non-feasible. Partial prevention occurs when the probability of occurance decreases. The set of initiating

conditions can be considered as a sequential condition, namely the sequential event that is just prior to the contingency. The reason one should attempt to distinguish the initiating conditions from other sequential conditions is: once the initiating conditions have occurred, the contingency can not be prevented if all other necessary conditions have been satisfied. In addition to this, the initiating condition can be used to initiate the immediate actions of the applicable contingency plan.

It may not be possible or profitable to prevent a given contingency on a permanent basis. If this is so, then one must consider contingency control and/or contingency planning.

A special (or familiar) type of prevention is accomplished by designing system "interlocks". Interlocks are designed to take advantage of either sequential conditions or necessary conditions that must occur simultaneously. By adding constraints to the system, one can prevent the occurance of one or more of these necessary conditions and thereby prevent the contingency from occuring.

Contingency Control

After all desirable efforts to prevent a contingency have been expended, then one's attention is directed towards totally negating the effect of the contingency before it occurs. In order to do this, security constraints must be imposed in order to insure that the system remains secure with respect to this contingency.

In the preceeding section, one form of contingency control was mentioned, namely terminating a contingency before it disrupts the system's structure. In general, any action taken before or during a contingency that attempts to negate the effect of the contingency is contingency control. If the contingency control is totally effective, then when the contingency occurs, the system will remain in a normal mode of operation. It is important to note the difference between prevention and control. When contingency prevention is totally effective, the contingency can not occur. In the case of contingency control, the contingency occurs but the system is being operated in such a manner to insure that the contingency does not disrupt the system's structure enough to cause an emergency. Thus the key to effective contingency control can be found by answering the following questions: can the system be operated in alternative modes of operation? If so, can one select an alternative mode of operation, in which the contingency under consideration will be less disruptive? And finally, are there modes of operation, in which the effect of the contingency is totally negated? That is, when operating in one of these modes, the contingency will not result in an emergency or damage. If it is not possible to totally negate the effect of the contingency before it occurs, then prevention is necessary and if neither total contingency prevention nor total contingency control has been implemented, then this contingency will result in an emergency when it occurs.

Now assuming that it will occur and that an emergency will be one of the results, it is logical to question how much damage will occur. Depending on the actions that are taken after the contingency has begun to occur, this damage will vary. Actions taken to minimize the damage should be part of a contingency plan.

Contingency Planning

In many cases, once the contingency begins to occur, some structural change is inevitable. In order to minimize the structural damage, selected groups of subsystems are quickly isolated from the overall system. This is accomplished by using fast-acting automatic protection devices, such as isolation valves, thermal and electrical fuses, circuit breakers and flow diverting devices. The automatic protection devices may have priorities, be sequentially ordered, be interlocked or be the initiating action of other contingencies and/or more complicated special protection systems. The purpose of the fast-acting automatic protection devices and other immediate actions is to reduce the extent of the structural damage, to put the system in a safe condition from which known recovery measures can be used to restore the system to normal, and to ease the recovery by preventing the occurance of unnecessary complications. Once the immediate actions have been taken and all automatic protection devices have actuated, then the system is in a fail-safe condition. At this time recovery procedures can be implemented and they include

shifting from a fail-safe condition to the maximum partial load condition. That is, one would like to restore all undamaged isolated subsystems to normal and connect these subsystems in a manner which will give the system a partial load capacity. This topology will satisfy the maximum number of customers according to a priority listing in which a lower priority consumer will not be satisfied until all higher priority consumers, that can be satisfied, have been satisfied. As damaged portions of the system are repaired, using a priority system of repair these subsystems can be placed in service to increase the partial load capacity. In this manner, the entire system will eventually be restored to normal, and will be capable of satisfying all the demands on the system. In some systems, the best contingency plan may be the plan that can get the system back to normal as soon as possible with a minimum amount of off-quality product.

When a contingency plan is needed, it is too late to be developing it. Prior to the contingency, the following should be known: the least desirable state of the system just prior to the contingency, the desired "fail-safe" condition for this contingency, and the desired normal mode of operation after restoration. Through knowledge of the system behavior and/or simulation, one can determine the transition of the system during the emergency. Without implementing the contingency plan, this transition begins with the least desirable state of the system and ends with the simulated state after the contingency.

Then the control problem is to formulate a sequence of actions which will cause this transition to terminate in the desired "fail-safe" condition. As a contingency begins to occur there may be doubt as to which contingency is occurring or where it is located. This is due to the fact that an initial portion of the transition for several different contingencies may be identical.

This necessitates a set of simple yet decisive diagnostic actions. The purpose of these diagnostic actions is to determine the following: which contingency is occuring and where it is located? The diagnostic actions are usually sequenced according to priorities. Sequential priorities can be based on the following facts: 1) There are vital subsystems which should be maintained in a normal operating mode as long as possible. 2) There is an optimal (minimum) number of diagnostic actions and by taking these in the proper sequence, the location will be determined in a minimum amount of time with the least amount of disruption to the normal mode of operation. 3) There are locations that are more likely to be the location of the contingency than others. These locations are determined on the basis of past performance and system design. 4) Each succeeding diagnostic action should depend on the results of preceeding diagnostic actions. Diagnostic actions can terminate when either the type and location of the contingency are known or when emergency actions are necessary to insure that the transition will terminate at the desired "fail-safe" condition.

To increase the time available for diagnosis and correction, certain stationary actions can be taken. The purpose of these stationary actions is to maintain the present state or condition without interfering with the diagnosis and allow more time for diagnosis. There are conditions beyond which no emergency actions exist which can insure a termination at the desired "fail-safe" condition. Before one of these conditions is reached, emergency actions must be initiated and at this time additional diagnostic or stationary actions will not be undertaken. Once actions are taken to force the system into a "fail-safe" condition, every action is devoted to this end. In addition to emergency actions, isolation and safety actions may be necessary to attain the "fail-safe" condition. When a "fail-safe" condition is reached, it must be verified. That is, one must determine that the desired condition has been reached and that it is a stable and safe condition. For example, a point of conditional stability is not acceptable as it is not usually safe.

Additional actions are necessary to take the system from the "fail-safe" condition to a partial load condition. These actions are recovery or restorative type actions and can be taken with care when time and the situation will permit partial restoration. These actions are often the reverse of the diagnostic, isolation and safety actions taken during the emergency. As the repairs are completed, transitions to other partial load conditions will be

permitted until the entire system is restored to normal. Since recovery actions from various "fail-safe" conditions have already been planned, the transition from one partial load condition to another can be accomplished safely by returning to a "fail-safe" condition and then using these tested pre-planned actions. This will eliminate the expense of developing plans between all of the various partial load conditions. In addition, the use of existing safe procedures for obtaining optimal loading for various partial loads demanded during the normal mode of operation will reduce the work involved in planning restorative actions.

Modes of Operation

As previously mentioned, as the internal structure of a system changes the mode of operation changes. This can result in a large number of topologies for the larger composite system. Each identifiable system topology can be considered to be a mode of operation for the system. The number of different modes of operation can be quite large, in fact, if instead of discrete modes for each subsystem, if any one subsystem has a continuous mode of operation where the mode can be altered in a continuous manner over a range of values, then there will be an infinite number of modes for this subsystem and an infinite number of modes for the composite system. If one desires to limit the modes and insure that there is a finite number of modes, then each continuous range can be divided into a finite number of increments.

Since this number will be large for a complex system, it is worthwhile to consider certain collections (sets) of these modes. For security control, a natural partitioning occurs if one considers those sets which are separated by the system constraints. Whenever the operating and load constraints are satisfied, the system is in one of the normal modes of operation. If either a load or an operating constraint can not be satisfied, then the system is in one of the abnormal modes of operation. There are three types of abnormal modes of operation: a set of alarm modes in which the operating constraints are not satisfied but the load constraints can be satisfied, a set of emergency modes in which neither the operating nor the load constraints can be satisfied, and a set of restorative modes in which the load constraints can not be satisfied but the operating constraints can be satisfied. This decomposition is natural because it is related to the condition of the system prior to, immediately prior to, during and after a system emergency.

In a normal mode the security control effort is devoted to contingency prevention and contingency control. In an alarm mode, additional security constraints are imposed in order to prevent the occurance of other contingencies and to reduce or negate the effect of the contingency that has begun to occur. Contingency prevention and contingency control for the other contingencies continue as before, unless this contingency is one of the necessary conditions for another contingency. In an emergency mode or a restorative

mode, the contingency has either begun to occur or has occurred and the control effort is devoted to the implementation of a contingency plan. The security control actions can be called preventative, corrective, emergency and restorative actions corresponding to the four sets of modes: normal, alarm, emergency and restorative.

Of particular interest is the security control actions associated with the normal and alarm sets of modes because in these cases it is possible to adjust the operation of the system by the imposition (and relaxation) of security constraints to enhance (and degrade) the security of the system.

Figure 2-1 depicts pictorially the relationship between the various modes of operation and the load and operating constraints for some hypothetical system. Security constraints have not been shown on this figure. In this figure the normal operating space is enclosed by a boundary.

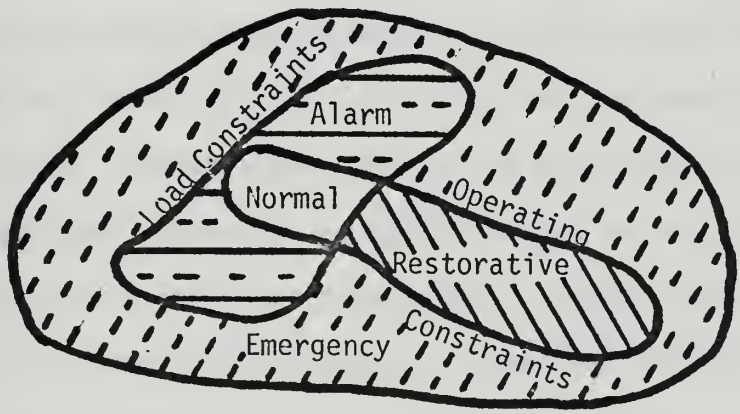


Figure 2-1

In order to remain secure one must operate the system in such a manner as to avoid violation of this boundary. Thus there are two mutually exclusive and collectively exhaustive subsets of this normal operating space (a secure and an insecure subset). Conceptually this is shown in Figure 2-2.

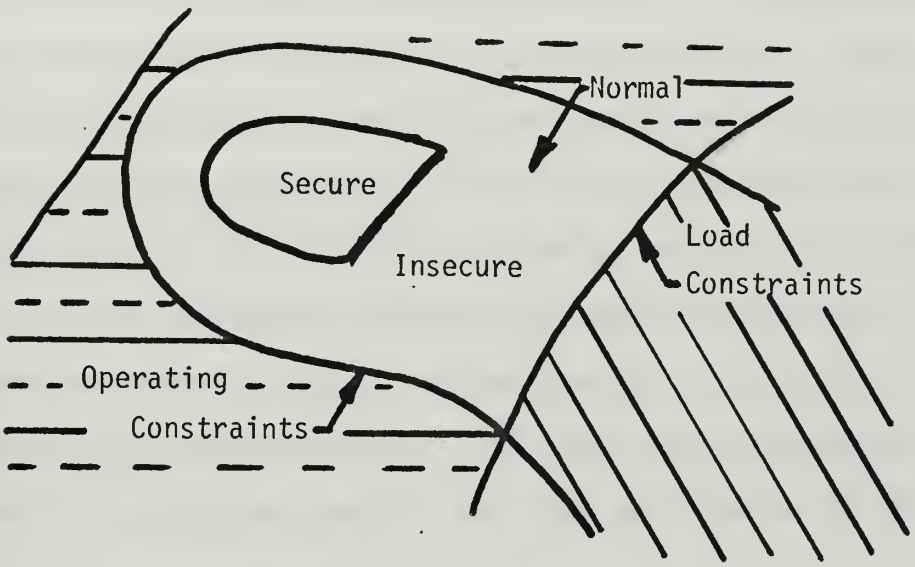


Figure 2-2

Once a "set of next contingencies" has been chosen the boundary of the secure region is fixed. This boundary is made up of the security constraints that are associated with a particular "set of next contingencies". Ideally one would like to be able to concisely enumerate these security constraints. If this can be done then the security control problem becomes a constrained optimization problem. For the case where the security constraints can not be enumerated, then this boundary must be estimated. When pattern recognition is

used to determine whether or not a system is secure or insecure, the pattern recognizer constructs an approximation to this boundary and then uses this approximation to determine whether an untested operating point lies interior or exterior to this boundary. The opposite approach is to exactly determine the boundary by listing the applicable security constraints. If this can be done, then the trade-off between security and performance can be defined exactly. Using this trade-off relationship one can determine when to impose and relax individual security constraints. This is what is being done by operators when they make decisions concerning security and performance. The most significant difference is operators make their decisions based upon experience rather than the solution of a constrained optimization problem. Thus their decisions may not be repeatable or consistent, and may vary from one operator to the next.

Now that the alternatives have been described a method of selecting which alternative should be implemented must be developed. In order to decide this, the cost of the various alternatives must be compared. This decision and the associated costs will be the subject of the next chapter.

CHAPTER III

COST OF SECURITY CONTROL

In this chapter the decision process for selecting security control alternatives will be developed. This decision process depends on the costs of these alternatives as well as many other factors. One should note the importance of the planning horizon. The decision to implement or not implement a security control action will depend directly on the planning horizon. For any given contingency, the total cost will be the sum of the costs due to contingency prevention, contingency control, and contingency planning.

Before considering any specific action, one must understand how to justify any security control action without specifying whether or not it is contingency prevention, contingency control, or contingency planning. Let L_{ref} be the penalty if a given contingency occurs without security control. Let P_{ref} be the expected frequency of occurance for this contingency in a given planning horizon. That is, if one expects the contingency to occur twice within this time period, then $P_{ref} = 2.0$. If one expects an occurance once in twice this amount of time, then $P_{ref} = 0.5$. Then the EMV (expected monetary value per unit time) of the loss without security control is:

$$EMV_{ref} = \frac{P_{ref} \cdot L_{ref}}{\text{Planning Horizon}}$$

Note:

$$EMV_{ref} \leq 0$$

The more negative the EMV, the larger the expected loss. This is the reference value for all security control cost decisions. Any control action (preventative, corrective, emergency or restorative) must reduce this weighted penalty by an amount greater than its cost (per unit time) in order to be justified. Let C_a be the cost (per unit time) of the action and EMV_a be the expected monetary value if the action is taken, then security control is justified if and only if the expected gain is greater than the cost of the action.

$$EMV_a - EMV_{ref} > C_a$$

If the cost of the action and the expected monetary value of the loss with the action are considered as variables which will depend upon the type of action taken, one can maximize

$$EMV_a - C_a - EMV_{ref}$$

in order to determine which action to take.

There are two special cases, namely total contingency prevention and total contingency control. In each of these cases, the EMV becomes zero. In the case of total prevention, it is zero because the expected frequency of occurance is reduced to zero. In the other case, the penalty is reduced to zero because the contingency

has been negated. In both of these cases, the cost (per unit time) of the action can be as high as the reference EMV and the justification criterion will still be satisfied. If either can be achieved, then a very simple set of Boolean decisions can be used to compare the costs with the reference. The result of this decision process will be either contingency prevention, control or planning but it will not be a combination of the actions. If neither total contingency prevention nor total contingency control can be imposed, then partial actions or contingency planning must be considered. When one considers partial actions, a combination may result in the greatest reduction of EMV at a minimum cost.

Thus, the decision process depends upon one's ability to evaluate the loss, the expected frequency of occurance, and the costs (per unit time) of the actions. As in most realistic decision processes, the EMV can be estimated if there is insufficient knowledge of the system to actually calculate the appropriate numbers.

Cost of Contingency Prevention

Contingency prevention usually requires additional equipment to monitor and regulate certain of the system parameters. This involves a capital investment and the imposition of additional constraints on the system. These constraints are operating constraints, for without them continuous operation may be in jeopardy. The cost of the equipment, installation, and operation are fixed

costs. Therefore, they do not affect the optimization. These costs must be divided over a period of time (the planning horizon). The new operating constraint will affect the steady state operating point and the performance if this constraint becomes an active constraint. If it is active, then the continuous reduction of performance must also be divided by the appropriate planning horizon. If it is inactive, it will not affect the desired steady state operating point, however new security constraints may be necessary to insure that this operating constraint is not violated. If this is required, it is contingency control and the cost (per unit time) of imposing and relaxing these security constraints must be considered under contingency control.

The Cost of Contingency Control

The cost associated with contingency control can be calculated in a straightforward manner. Since contingency control requires the imposition and relaxation of security constraints, the overall system performance index can be used to calculate the cost. If one solves the optimization problem with and without the security constraints for a given contingency, the corresponding operating points will have indices of performance associated with those points. The cost of contingency control for a given contingency is the difference between the performance with and without security constraints. Thus, security with respect to each contingency can be evaluated on its own merits.

It is important to note that the expected frequency of occurance may vary as a function of the operating point. If this is the case, then the decision to implement contingency control for a given contingency becomes a dynamic decision-making problem, requiring a measurement or estimation of the current operating point. If this is the case, both reference EMV and the action EMV will vary as a function of the operating point. This requires that the contingency control problem be updated and re-evaluated periodically. This is a higher stratum feedback mechanism that resembles normal feedback control. This will be explained in greater detail in chapter six.

Cost of Contingency Planning

If there is any reason to believe that the contingency will occur and result in damage in spite of efforts to prevent it or negate the effect of the contingency, then a contingency plan is needed to reduce the penalty (damage). Note that the decision is not whether a contingency plan is needed but how elaborate a plan can be afforded.

The actions to be taken can be divided into two types, those that depend upon only the contingency and those that depend upon the contingency and the operating point of the system. The first type constitutes the framework of the contingency plan and the others are appended to this framework according to the situation. The cost of the framework actions can be neglected as these actions will be taken if the contingency occurs and the damage is to be

minimized. It is no more costly to develop them in advance than to develop them as the contingency occurs. Usually it is less costly. In the case of the second type, the actions can be developed in advance for many situations, can be developed in advance for only the worst situation, or can be developed for a few typical situations. The necessary simulation and computer programs can be developed without working out actions for any particular situation, or the planning can be neglected in favor or reliance upon the training and ability of the operators. Clearly, a large risk (expected frequency of occurance) and a severe penalty will justify more pre-planning and training. The framework actions require very little simulation since they are often based upon the macro-characteristics of the system. On the contrary, the details of the appended actions often require accurate and costly simulations. Assume that one can estimate the cost (per unit time) of any portion of the contingency plan. Then to justify this portion of the plan the EMV must be increased by an amount greater than this cost.

In conclusion, it is important to note that if the contingency can not be prevented or negated then a loss will occur as a result of the contingency. This establishes a reference standard for making decisions concerning security control. That is, the weighted penalty (EMV of the loss) which will result when there is no security control is the reference and to justify any security control it must reduce this weighted penalty and the cost must be less than or equal to the

the penalty reduction. This will insure that the sum of the new EMV and the total cost is less than or equal to the original weighted penalty (the reference EMV).

CHAPTER IV

EXAMPLES OF SECURITY CONTROL

In the next three chapters several examples of security control will be presented. The purpose of these examples is to illustrate the applicability of security control to familiar industrial situations. However, this does not imply that security control is limited to industrial systems. The concepts developed in this research can be applied to almost any system. Application appears to be easier on those systems to which multi-level control techniques have been applied. For these systems, all of the levels of control need not be fully developed. This will become more apparent in chapter six, where security control is applied to a system previously subjected to only direct control. This chapter will describe the glass manufacturing process, contingencies that threaten this system and areas were security control can be applied. The emphasis is on the applicability of security control. Some of the contingency control examples have been deferred to a later chapter, where they will be discussed in greater detail.

In Figure 4-1, the glass manufacturing system has been illustrated in a block diagram form. This is, of course, an oversimplified representation.

As shown, previously ordered raw materials of acceptable quality are received in bulk quantities. Each material has its own peculiar

The Glass Manufacturing Process

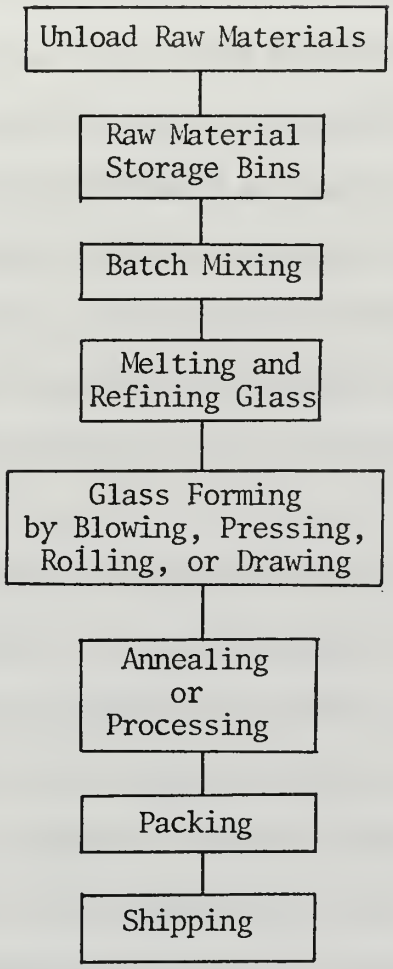


FIGURE 4-1

characteristics and hence must be packed, unloaded, processed, stored, and mixed in a distinctive way. These raw materials are transferred to storage bins, which have been designed to prevent contamination, caking and other environmental changes. The raw materials are precisely measured as they are removed from storage and accurately weighted prior to transfer to the mixer. Upon completion of the mixing, the dry batch is transported to intermediate storage and then to the rear of the glass furnace, where it is automatically and continuously fed into the melting end of the furnace.

The glass furnace is separated into two distinct ends, a melting end and a working end. A rotating auger is often used to feed the batch mixture into the melting end where it is melted by the roaring jets of flame that shoot across the top of the pool of molten glass. The melting end is separated from the working end by a bridge wall that has a throat at the bottom which allows the properly refined and partially cooled glass to flow into the working end. In the working end, the glass in a vitreous state cools to the desired working or gathering temperatures. While cooling, the bubbles continue to fine out.

Connected to the working end are numerous forehearths, which are used to maintain the glass at the proper temperature for gathering and working. Automatic glass feeding machines, utilizing conditioned glass from the forehearth, produce gobs of glass of a predetermined

size, shape and temperature for the glass working machinery. Glass working includes a vast variety of methods and techniques such as blowing, pressing, casting, drawing and combinations of these. For process control purposes, it is sufficient to recognize that the glass working dictates the desired physical state of the glass entering the working device and that upon leaving the device the physical state of the glass, although changed, is fixed and specified.

After the glassware is shaped by the glass working machines, it is in a semi-finished state and must be either rejected, stored or finished. Finishing means cracking the object off, then smoothing any rough edges (by grinding and fire polishing) and then annealing to remove any unequally strained conditions. In annealing, the object is heated in a lehr to some constant temperature in the annealing range. At this temperature, most of the strain is relived by viscous flow and then the object is slowly cooled in order to prevent the introduction of any new strains. After annealing, the glass object may require decoration. Decorative processes include etching, sand blasting, cutting, engraving, enameling and various methods of coloring the glass with designs. After the decorating has been completed, additional firing may be necessary in order to make the decoration permanent. After this, the product receives its final acceptance (or rejection) inspection. If the glassware passes the final inspection, it is packaged and then shipped to the customer.

The overall objective of the glass manufacturing process is to produce glassware according to customer demand (orders). That is, produce the required number of each specified type of glassware, on or prior to a delivery date. Economically one would like to produce the glassware at a minimum cost. Once a production line has been set up and started, the glassware will be produced at minimum cost if the production line can be kept in continuous operation, and the number of rejects can be minimized. The minimization of the percentage of rejects can be accomplished by selecting plant operating parameters that maximize throughout subject to quality control constraints. In order to keep the production line in continuous operation, one must analyse those contingencies that are capable of shutting down the production line. One is definitely interested in the contingencies that can damage the production process and thereby increase the downtime and the financial loss occurring as a result of this downtime. In addition to these, contingencies that can cause the plant parameters to be out of specification (resulting in poor quality glass) must be considered.

The contingencies of particular interest are those which jeopardize production, the rate of production or delivery dates. Some of the contingencies that have been realistic contingencies for the glass manufacturing process can be listed as follows:

Inventory Outage

Mixer Failure

Constituent Separation

Batch Hopper Hoist Failure

Auger Failure

Glass Tank Contamination

Glass Tank Leakage

Loss of a Major Utility

Loss of Temperature Control

Stirring Rod Failure

Loss of Flow Rate Control

Glass Feeding Machine Failure

Glass Working Machine Failure

Conveyor System Failure

Improper Quality Control

Loss of the Finished Product Removal System

There are other contingencies which have not been listed. Their omission does not imply that they are less significant, only that they are less obvious. It is worthwhile to consider each of these that have been listed in detail.

An inventory outage at any point in the production line can either halt production or reduce the overall rate of production. If the inventory is of a raw material that is common to all glasses then all of the glass furnaces could eventually be brought to an idle condition. If it is a raw material that is used for only cer-

tain specialty glasses, then the outage may only affect one glass furnace. There are numerous holding or storage facilities that act as surge tanks in the system. However, a sustained outage will eventually deplete one or more of these reservoirs. An inventory outage is not restricted to raw materials at the batch end of the process. For example, if there is an inventory outage of packing material used at the output of the system, or a decorating color used at an intermediate point on the conveyor system, the stacking up of semi-finished and finished products would soon bring the conveyor system to a halt.

Throughout the glass manufacturing process there are vital pieces of equipment. If one is damaged or fails to operate properly the process will be brought to a standstill until it can be repaired. For example, at the mixing facility there is often only one mixer. Behind each furnace is a hoist for moving the batch hoppers into position. At the rear of each furnace is an auger for feeding the mixer batch into the furance. If any of the previously mentioned items fail and can not be replaced or repaired within a certain time duration, the glass furnace and all of the production lines being fed by that furnace will become idle. Downstream of the furnace there are pieces of equipment that are vital to the production line in which they are located. For example, after each forehearth is a stirring assembly. Feeding each production line is a glass feeding machine. Downstream of the glass feeding machine are a whole series

of machines, conveyors, motors and other devices that are connected in series. Together they constitute the glass working, annealing and finishing systems. These systems are connected continuously and can be called the conveyor system. Failure of any element in this conveyor system would bring the individual line to an idle condition and reduce the overall rate of production. This illustrates two different types of vital pieces of equipment, one which is vital to the entire process and the loss of which is capable of reducing the overall production rate to zero and the other which is vital to a parallel subsystem of the process and if lost is capable of reducing the production rate of that subsystem to zero.

Continuing with the individual contingencies, the next to be considered is product contamination. The most obvious source of contamination is the introduction of either the wrong materials or the wrong amount of materials prior to mixing. If the constituents of a dry batch separate, the mixture becomes "unmixed". If this unmixed batch is introduced into the furnace, the glass which is produced may have cords and seeds. It is possible to introduce a batch hopper that was destined for a given furnace into the wrong furnace causing the entire contents of the furnace to become contaminated. This contingency differs in magnitude from the introduction of the wrong materials or contaminates into the batch prior to mixing. Both result in bad glass that may not pass the required quality control inspections. The other source of contamination is the erosion of

the refractory material that is used for the construction of the furnace. This erosion not only produces contamination and stones, but it can lead to a glass leak.

There are several contingencies that affect the entire process or can occur throughout the process to one degree or another. All of the system parameters that are being controlled by direct controllers have certain limits within which these parameters must be maintained for either component, system or personnel safety. A failure of any one of these control systems constitutes a threat to the continuous safe operation of the manufacturing process. In addition there are certain utilities which are being used by every portion of the process such as electricity, water, gas and air. A loss or partial loss of one or more of these utilities can be catastrophic to the process. Yet these utilities can be services that are provided by an external source, and there is no guarantee that they will be provided continuously.

Now that the most obvious contingencies have been discussed, they can be divided into the following categories: inventory outage, product contamination, loss of a vital component, loss of a control system, and loss of a major utility.

After studying the glass manufacturing process and its numerous disruptive disturbances, one becomes aware of the large number of potentially dangerous contingencies that can be quickly found in any industrial process. This is especially true where the performance

is directly dependent upon the continuous operation of the process. How can these contingencies be handled? In general, there is no simple answer to this question. Each contingency must be analysed separately and a determination must be made concerning whether to apply contingency prevention, contingency control, contingency planning or some combination of the three. That is, one could try to prevent them. If they can occur in spite of our efforts to prevent them, then there are two more alternatives to consider. One can insure that the system is secure before the contingency occurs and thus insure that the system can continue to satisfy load and operating constraints. If the contingency can not be prevented and the system can not be made secure with respect to this contingency, then one can be ready to take action to minimize losses as soon as the contingency occurs.

In the glass process as it evolved over the years, many of the contingencies that can be prevented, have been prevented by redesign of the system. This redesign resulted in the permanent imposition of certain constraints. These constraints together with the load (mostly quality control) constraints have rigidly fixed most of the system parameters. This rigidly controlled system has fewer modes of operation and thus fewer alternatives when one considers security control. In this and other rigidly controlled systems, security analysis will often result in additional preventative measures and contingency plans for those contingencies that can not be prevented. Contingency con-

trol will be the exception rather than the rule, as the system is already over-constrained by the existing constraints. When a system is over-constrained, only a single operating point exists rather than a feasible operating space. Security analysis may indicate where some of these constraints can be relaxed in order to achieve an improvement of either quality or performance. If this can be done, then contingency control will be necessary to relax and impose security constraints as needed. The glass process yielded examples of all three methods of security control. The description of the application of contingency control to this process will be covered in the next chapter, "EXAMPLES OF CONTINGENCY CONTROL". The examples of contingency prevention and contingency planning will be discussed in this chapter.

Inventory Outage

The inventory outage can be prevented. However, the prevention requires tying up capital in increases inventories. Rather than completely preventing inventory outages, the decision is often made to reduce the capital investment in inventories and try to establish an inventory level which will insure that the system is secure with respect to this contingency, inventory outage. The contingency or disruptive disturbance is actually an unexpected demand or a delivery failure. The outage is a result of this disturbance. The adjustment of this inventory level becomes a trade-off problem be-

tween security and performance. This can be handled as a contingency control problem. In this particular problem, the contingency control appears almost as on-line contingency prevention. If the contingency is not totally negated, then some form of contingency planning will be necessary.

Product Contamination

For the most part, product contamination in the glass manufacturing process can be prevented more economically than it can be controlled or corrected. Contingency control involves a feedback loop that uses quality control information to change the constituents being introduced into the glass furnace. Correction after the contingency requires shutting down the production line, flushing, and restarting the production line.

Quality control specifications and inspections of the raw materials received can preclude the introduction of substandard materials into the storage bins. The frequency of quality control inspections will differ with each material both because of the quantity used and the likelihood of receiving substandard material. Realistic specifications will reduce the probability of receiving substandard material and thus reduce the number and cost of the inspections.

In the case of contamination introduced by the mixing of the wrong materials or the wrong amounts of raw materials, the error

is difficult to detect until the finished product is given final quality control insepctions and tests. Thus, by the time the error is detected, the contingency has already occurred. To prevent this contingency, the material handling system can be modified to make it almost impossible to cause contamination. To assist in this effort, a computer-aided material accounting system could keep track of the flow of materials. A periodic automatic auditing would detect possible contamination before it could become a serious problem. Additional quality control inspections might be initiated or requested based on the results of the computer auditing. If the contingency occurs and is detected during routine quality control inspections of the finished glassware, then a contingency plan need only consist of a method of determining if additives can correct the deficiencies of the glass in the furnace. If not , then the production line must be shut down, the furnace emptied and flushed, and the line restarted. If so, then the additives must be introduced into the furnace and the glassware being produced must be scrapped as cullet until it can pass the quality control inspections. This feedback loop has an extremely long time constant. However, by introducing a computer into this loop, the materials being introduced into the furnace can be altered in response to the quality control inspections. This would reduce the number of shutdowns required, especially if the contamination is gradually increasing. This same computer-aided quality control feedback loop can be used to compensate

for the contamination introduced by the erosion of the furnace refractory materials.

Contamination resulting from the introduction of a given batch into the wrong furnace can be prevented by either using color or shape coded transportation facilities. By using hoppers of either different shapes or different sizes, one can make it impossible to introduce a hopper into the wrong furnace. This is similar to building interlocks to prevent contingencies. An alternative method of prevention is the creation of a contained system. Once the system is contained, then only the integrity of the boundaries need to be maintained. Again a computer-aided transportation system can keep track of the movement of materials and assist in maintaining the integrity of the boundary. For example, an identification card would accompany a batch as it moves through the mixing process and then through the plant. The computer would keep account of the materials added to the mix. If this mixture was incorrect, a gate regulating entry to the rear of the furnace would not open for the wrong type of mix. This type of system would be warranted if the losses involved in furnace contamination were large enough. In certain high quality specialty glasses this is the case, for a contaminated furnace can not be corrected but must be shutdown, flushed and restarted. Since the greatest cost is the downtime and the loss of production, this can be minimized by developing a sequence of actions (a contingency plan) to shut down, flush and restart this

furnace in a minimum amount of time.

Contamination caused by batch separation can also be prevented, when warranted. Separation occurs because certain necessary conditions are present, namely agitation and space between constituents. The agitation can be reduced and the space nearly eliminated by compacting the mixture. If compacted into a shape which would optimize the melting process, these compacted units could be introduced on a continuous basis. The material handling system between the mixing facility and the furnace could be redesigned into a continuous system to take advantage of these compacted units.

Loss of a Vital Component

Some components can be replaced or repaired in a relatively short period of time. If there is an inventory following this type of component and the intentory can be maintained above some minimum level, then the overall system can be made secure with respect to the loss of this component.

Contingency prevention for the loss of a component involves component upkeep and preventative maintenance. The scheduling of maintenance during scheduled downtime is common practice in many industries. The unexpected loss of a component indicates that this preventative maintenance needs to be re-evaluated. Periodic updating of maintenance techniques and maintenance schedules is an effective means of insuring safe and continuous operation of vital

components. Some of the vital components, such as motors, change their characteristic vibrations as the probability of their failure increases. By using vibration analysis techniques, these changes can be detected and maintenance and replacement schedules altered accordingly. This example of contingency prevention is of special interest when one considers the justification aspect of this problem. The cost of replacement, the EMV after the action, and the reference unweighted loss are fixed. Only the reference expected frequency of occurance is changing as a function of time, and this change can be measured. By applying the cost criterion of chapter three, one can determine the appropriate time for motor replacement. One minor difference is the desire to accomplish the replacement during a scheduled downtime. This will require a projection of the cost criterion from one downtime to the next (predictive security control). If the criterion will be satisfied in the next operating period, then the projected change of the reference expected frequency will determine if the motor must be replaced before the next operating period. If the system under consideration were mobile (for example, a space craft, an airplane, or a submarine) it might be impossible to replace a vital component during an operating period.

Some of the vital components have multiple modes of operation. Contingency control can be used to select the mode of operation which will best negate the effect of the contingency. A good ex-

ample of this in the glass manufacturing process is the operation of the stirrer assembly that follows the forehearth conditioning section. The contingency or disruptive disturbance is an unexpected increase in glass viscosity, due to perhaps a loss of temperature control in the forehearth. By changing the speed of this stirrer, excessive torques can be avoided and stirrer failure can be eliminated.

Many vital components do not have alternative modes of operation and in spite of maintenance efforts will eventually fail. To be prepared for these failures, contingency plans are needed for changing the operation of the unaffected portion of the process, repairing or replacing the damaged component and restoring the process to normal. These contingency plans can include automatic protection devices for the individual components as well as the overall process.

The following is a description of a contingency plan that can be implemented by the use of an automatic protection device. In a glass manufacturing process containing a glass pressing machine, gobs of molten glass are fed into the female half of a mold by the glass feeding machine. The other half of the mold then presses the glass into the desired shape. The hot glassware may be subjected to additional working and fire polishing before it is removed from the mold. Eventually a vacuum device lifts the molded glassware from the mold. The mold cools for a short period of time and is returned to receive another gob of molten glass. If for any reason the molded

glassware is not removed, a very serious contingency has occurred. The mold is being positioned by an automatic pressing machine. When it is positioned under the gob chute, the molten gob of glass will be deposited in the glassware instead of into an empty mold. Then when the pressing action occurs, the mold will be destroyed. In this case, contingency prevention entails design improvement and better control of the vacuum lifting device. In spite of these efforts, the contingency can still occur. To monitor when it has occurred, an optical pyrometer can be installed to view the mold cavity after it passes the vacuum lifting device. When the mold is empty, one temperature will be recorded. When the glassware has not been removed, a distinctly higher temperature will be recorded. This contingency can be detected before the damage occurs. An electrical-mechanical device can be constructed to divert the gob chute. Whenever the mold is not empty, the gobs of molten glass will be diverted to a cullet hopper. As soon as the glassware has been removed, the system can be restored to normal. This can be accomplished by operating personnel or by automatic devices which react to a reset signal. The importance of this example is to point out that contingency plans can be automated and when this is accomplished, the device which carries out the immediate actions is a special purpose automatic protection device.

Loss of a Control System

The contingency resulting from a partial or total loss of a

control system can be handled by the system designers. Most control systems have or can be provided with alternative methods of control. The important aspect of this contingency control is that sufficient measurement and detection equipment must be installed to indicate to operating personnel when a given method of control is inadequate. The indication to change the mode of control must be clear and decisive. If this is the case, then a well-designed alarm system can present the conditions and the alternatives.

If the dominant response is slow enough, the mode of operation can be shifted before the contingency occurs and thus this is a form of contingency control. In some proecesses, the mode of operation will be shifted automatically by fast acting automatic protection devices. In this case, these devices are automated contingency plans. As a control system becomes more complicated, more alternatives can be provided to handle partial or total failure of that control system. The decision of which mode should be selected depends on the condition or state of the process and the nature of the failure. In order for the system designer to determine whether adequate alternatives are available, he can assume that all or any portion of the control system can fail and if sufficient means are available to carry out the applicable contingency plan, then the alternatives are adequate. If the alternatives are not adequate, then simulation will indicate the performance of the system in the absence of this control system.

The simulation will also indicate when a "fail-safe device" is needed. An example of such a device designed for this purpose is the provision of automatic "scrams" on a nuclear reactor.

Loss of a Major Utility

The contingencies that involve the loss of a major utility are different in the sense that these utilities are often provided by an external system not under the jurisdiction or control of the glass manufacturer. It is difficult if not impossible to instrument and monitor this external system in order to be able to predict or prevent a loss. The effects of this contingency are often catastrophic and compounded due to the lack of experience in handling this type of casualty. The loss is usually sudden and without warning. Even if a back-up or alternative system is available, it is used after the contingency occurs. Since the loss can not be prevented or controlled, the remaining alternative is to provide contingency plans that are based on the experience of operating personnel and the knowledge of the system designers. The actual contingency plans that were required by the glass process for loss of a major utility varied from quite simple to extremely complex. It may be necessary to automate the more complex plans, either with automatic protection devices or a computer system. The proper sequencing of actions, timing, and the assignment of customer

priority (for the particular utility) are very important aspects of these plans. Regardless of how they are carried out, there is a sequence of actions to be taken that will minimize losses.

In summary, this chapter has demonstrated that contingencies exist in an industrial system and that security control actions for these contingencies can be developed. For each contingency, the actions of contingency prevention and contingency planning were identified and separated. Contingency control was only applicable where the operating space consisted of more than one operating point. In those cases, where contingency control could not be applied, the single mode of operation (operating point) was determined by the load and operating constraints on that subsystem.

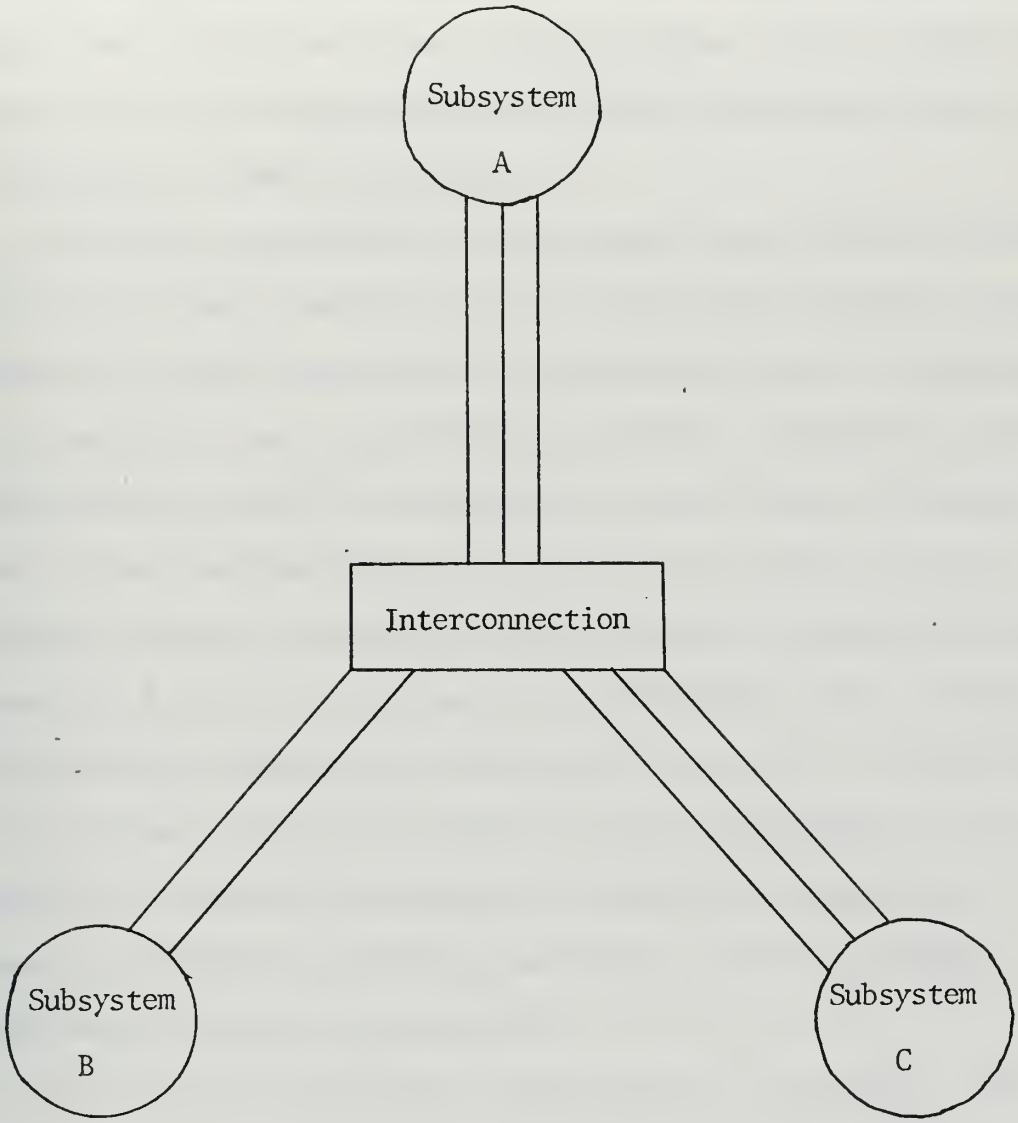
CHAPTER V

EXAMPLES OF CONTINGENCY CONTROL

In this chapter, emphasis is on examples which have operating spaces rather than a single operating point. An operating space is a collection of feasible operating points. When this set has only one feasible operating point it will be referred to as a "single operating point." Contingency control, the imposition and relaxation of security constraints, can be applied to these examples. The examples have been chosen to illustrate the concepts of security control in a variety of systems. The most significant point to be demonstrated is the existence or origin of security constraints and the relationship of these constraints to the operating and load constraints of a given system.

Power System Example of Contingency Control

Let us first consider an example which is typical of those systems that can be characterized by a complex network that connects a number of sources and a number of sinks. In particular, consider the following electrical power distribution network: three subsystems connected through an interconnection, shown in Figure 5-1. In this system, subsystems A, B, and C are each individually capable of satisfying more than the load demands in their region. The purpose of the interconnection is two-fold, economics and security.



Electrical Power System

FIGURE 5-1

By buying and selling power between the subsystems, the overall system can be operated more economically. In addition, when one of the subsystems is experiencing an internal problem, the other subsystems can assist by providing power and thus make the overall system less susceptible to these disturbances.

To clarify the necessity of contingency control for this electrical power system, consider this system under the following conditions: assume the power being produced by subsystems A and C is considerably less expensive than the power being produced by subsystem B, and the interconnection lines to subsystem B are each capable of carrying half of the load demanded of subsystem B. The solution of the economic dispatch problem under these assumptions would dictate that subsystem B buy all of its power from subsystems A and C and that the generating capability of subsystem B be secured. Of course this is an extreme, but for the purposes of this illustration, it is realistic. Now with the generating capability of subsystem B secured, consider the following contingency, loss of a single interconnection line to subsystem B.

Prior to this contingency, conditions were as follows: the system was in a normal mode of operation, subsystems A and C were providing all of the power to subsystem B, both interconnecting lines were loaded to capacity. Immediately after the loss of one of the interconnecting lines, the total load being demanded of the subsystems A and C will not change. However, all of this load will

be demanded over the remaining interconnection line. Since the unaffected interconnection line was previously at its capacity, in an attempt to carry this load, it will exceed its operating constraints. As soon as the operating constraints have been exceeded, the system will be in an alarm condition. If this condition is not immediately corrected, damage to the remaining unaffected interconnection line will result. There are two safe alternatives. In order to unload this interconnection line, one can either shed loads or isolate the line from the rest of the system. Usually the time required to shed loads is too long as compared to the time until damage occurs. Thus, in most power systems the second alternative is carried out. Overloads are handled by fast acting automatic protection devices. When the automatic protection devices isolate this interconnection line, the total load demanded of A and C will be reduced by an amount equal to the loads of subsystem B. All of the operating constraints can now be satisfied; however at least one of the load constraints can not be satisfied. Unfortunately subsystem B has been isolated from the remainder of the system, and its generating capability has been secured. The load constraint that specifies satisfaction of loads for subsystem B can not be satisfied. Any immediate attempt to restore power to subsystem B, without shedding loads, will result in overloading either the undamaged interconnection line, the generating capabilities of subsystem A and C or both, depending on how this restoration is

attempted. After loads have been shed, subsystem B can be restored to a partial load condition. Hours later, when either the generating capacity of subsystem B is ready to assume the load, or the interconnection line has been repaired, the load constraints on subsystem B can be satisfied.

Were there alternative modes of operation, in which this loss could have been prevented? There were many alternative modes. Subsystem B could have been operated with its full generating capability carrying its own loads. This is the most secure and the least economical mode, when one considers only the loss of a single tie line. Subsystem B could have been operated at a partial load capacity with or without spinning reserve. As long as the partial load plus the spinning reserve was equal to half of the load demanded by subsystem B, the system will be secure with respect to this contingency. For this example, the most economical yet secure mode of operation would have been to have subsystem B idling with a spinning reserve equal to half the load demand of subsystem B. In this mode of operation when one of the interconnection lines is lost, the generators of subsystem B will be required to immediately assume half of the loads of subsystem B, while the remaining half is supplied by A and C over the unaffected interconnection line. In stating that this is the most economical yet secure mode, the very important question of transient stability of this system was not described or investigated. For example, can this particular

subsystem be required to change from an idling condition to half capacity in a very short period of time?

The more general problem of security of this power system with respect to the loss of a single interconnection line can be developed in the following manner. In this example, the notation can be simplified by using vector notation. However, the origin of the security constraints for the contingency (loss of a single interconnection line) is not quite as obvious in the vector notation. In order to analyze this system, one can isolate each subsystem.

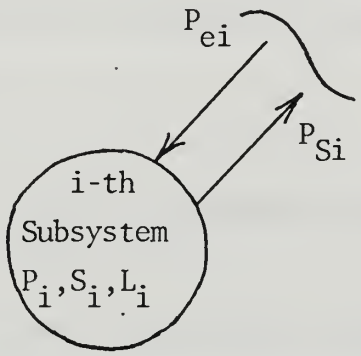


FIGURE 5-2

Then for each subsystem I, let

P_i be the power being produced by subsystem I.

S_i be the spinning reserve of subsystem I.

P_{ei} be the power being bought from an external source by subsystem I.

P_{si} be the power being produced and sold to an external subsystem by subsystem I.

The corresponding costs are

C_{pi} the unit cost of producing power internally

C_{si} the unit cost of maintaining spinning reserve

C_{pei} the unit cost of buying power

C_{psi} the unit additional cost of the power being sold to an external customer (This includes the profit plus the cost of distributing this power.)

$C_{pi} + C_{psi}$ the unit cost to an external customer

C_i the total cost of operating subsystem I

If the load of subsystem I is L_i then there are certain relations for each subsystem.

The load of each subsystem must be satisfied.

$$P_i + P_{ei} - P_{si} = L_i$$

For this illustration, assume that a subsystem will not buy and sell power simultaneously.

$$(P_{si})\ (P_{ei}) = 0$$

For systems that buy and sell power simultaneously this constraint

will not be applicable.

Each subsystem has some maximum generating capacity.

$$0 \leq P_i \leq \alpha_i$$

The sum of the power produced and the spinning reserve of a subsystem can not exceed the maximum capacity.

$$P_i + S_i \leq \alpha_i$$

The total cost of operating subsystem I is equal to the power production costs minus profits from selling power.

$$C_i = C_{pi} P_i + C_{si} S_i + C_{pei} P_{ei} - C_{psi} P_{si}$$

The maximum power that can be bought or sold is limited by the sum total of the capacity of the interconnection lines into subsystem I.

$$P_{ei} \leq \beta_i \text{ and } P_{si} \leq \beta_i$$

where

$$\beta_i = \sum_j \beta_{ij}$$

and β_{ij} is the capacity of the j-th interconnection line into subsystem I. Each subsystem at full capacity is capable of satisfying its own loads.

$$L_i \leq \alpha_i$$

If one considers the optimization for a subsystem without security then

minimize

$$C_i = C_{pi} P_i + C_{si} S_i + C_{pei} P_{ei} - C_{psi} P_{si}$$

subject to $P_i + P_{ei} - P_{si} = L_i \leq \alpha_i$

$0 \leq P_i \leq \alpha_i$

$0 \leq P_{ei} \leq \beta_i$

$0 \leq P_{si} \leq \beta_i$

$(P_{si})\ (P_{ei}) = 0$

In the previous description, the total capacity of the interconnection lines into subsystem B was equal to the capacity of subsystem B, and the cost of buying power was much less than the cost of producing power.

$$\alpha_B = \beta_B$$

$$C_{peB} << C_{pB}$$

Unfortunately the cost of the power being sold is always greater than the cost of producing that same power.

$$C_{pi} + C_{psi} > C_{pi}$$

All of the subsystems buy power from the interconnection, which in turn buys power from the subsystems that are able to produce power must economically. In this example, the interconnection will not buy power from subsystem B. Hence the solution to the economic dispatch problem will be

$$P_{SB} = 0\ ,\quad P_B = 0\ ,\quad P_{eB} = L_B \text{ and } S_B = 0$$

and the cost for subsystem B will be C_B .

$$C_B = C_{peB} \cdot L_B$$

Any other solution with $P_B > 0$ or $S_B > 0$ will result in increased costs. Now in order for subsystem B to be secure with respect to the loss of either interconnection line an additional security constraint must be added to this set of equations, namely.

$$P_B + S_B \geq \beta_{B/2}$$

This will make subsystem B secure with respect to this contingency. In this particular case, it was assumed that

$$\beta_B = \beta_{B1} + \beta_{B2} \quad \text{and} \quad \beta_{B1} = \beta_{B2}$$

In general, this subsystem security constraint will be of the form

$$P_i + S_i \geq \max_j \{\beta_{ij}\}$$

and β_{ij} is the capacity of the j-th interconnection line into subsystem I.

Now the I-th subsystem is secure with respect to a loss of one of its interconnection lines, but what about the remainder of the system? If subsystem B were supplying power instead of receiving power then there might not be sufficient spinning reserve in the remainder of the system to handle this contingency. This can be remedied by using another security constraint which insures the security of the rest of the system namely.

$$\sum_{\substack{\ell \\ \ell \neq i}} S_\ell > \beta_{ik}$$

where

$$\beta_{ik} = \max_{j} \{\beta_{ij}\}$$

To handle the interconnection of these subsystems one can insure

$$\sum_{i} P_{ei} = \sum_{i} P_{si}$$

There are many elements of this example which are present in most security control problems. For instance, the following were described: operating and load constraints, the optimization problem with or without security, the trade-off between security and performance, the existence of security constraints to insure security, the various modes of operation and their associated classes (normal, alarm, emergency, and restorative), and the existence of redundant capabilities. Of course, only one contingency (that might belong to the set of next contingencies) was considered. In the security analysis of a complex system all of the contingencies that are in the set of next contingencies must be enumerated and then developed in a similar manner. An equally difficult question is: how can one decide which contingencies should be in the set of next contingencies (those contingencies with respect to which the system must be secure)? A thorough and complete analysis of this problem for the electrical power system was recently completed by Tomas E. Dy-Liacco (12). However instead of finding the security constraints for each of the contingencies in the set of next con-

tingencies, Dy-Liacco used pattern recognition to identify whether or not the system was secure or insecure. In a sense, the pattern recognition scheme constructs a boundary which is an estimate of the hypersurface formed by the entire collection of security constraints. By constructing this boundary the complex problem of security analysis and the enumeration of the individual security constraints can be avoided. However, in this approach, only the Boolean answer of secure or insecure was available. In many systems, this Boolean answer is not only sufficient but is the only information needed for safe, secure operation of the system. In these or other systems, simulation can be used to predict whether or not any particular action or event will cause the system to become insecure. A combination of these two approaches can be used. The pattern recognizer can be used to estimate the boundary based upon the information available. Then, the optimization can be carried out subject to the operating and load constraints and also subject to the artificial security constraint developed by the pattern recognizer.

In the next example, security control will be applied to a portion of a production line in continuous operation. Recall that security control involves three approaches to a contingency (contingency prevention, contingency control and contingency planning). This example will be used only to illustrate contingency control. The process to be examined is a portion of the glass manufacturing process which was described in chapter four. This example was chosen

to illustrate how a system with a single operating point can be developed into a system with an operating space.

Contingency Control in the Glass Manufacturing System

The portion to be considered for contingency control is traditionally called the forehearth. However this consists of four distinct sections: a cooling section, a conditioning section, a mixing section, and a platinum tube that delivers the conditioned glass to the glass feeding device. Typically the cooling and conditioning occurs in a covered open channel whose dimensions are about 26 inches wide, 6 to 7 inches deep, and 18 feet long. The molten glass enters the cooling section at a temperature near 2400 degrees. Cooling is controlled by adjusting the burner-flame level and the amount of cooling air in the cooling zone. In the conditioning section, the walls have electrical heating elements and the surface of the glass can be heated by flames from above. In this section, the cooling rate is regulated by the combined use of the burners and the resistance elements. An attempt is made to deliver the glass to the mixing section at a nearly uniform cross-sectional temperature. Additional homogenity is achieved by stirring this conditioned glass in the mixing section. This glass must then be delivered to the glass feeding device. Delivery is accomplished via a platinum tube. Since this tube may be as long as 150 to 200 inches, it provides a final opportunity to finely control the temperature of

the glass. In this example, the final conditioning and temperature control is achieved by regulating the power to six sections of electrical heating elements which surround the platinum tube. The glass is delivered to the glass feeding machine which produces a gob (a discrete mass of molten glass created by intermittently shearing the stream of glass emerging from the orifice). This gob then free falls into a chute and is guided into a mold in the pressing or forming machine.

The glass forming machine needs a gob of a particular size, temperature (viscosity), and glass composition. Once the physical properties and the composition are specified, then the constituents used in the batch mixing process and the techniques of the melting and fining process will be specified. Since the rate of operation of the forming machinery is fixed by quality control considerations, then the shearing frequency will be specified. In order to achieve the correct size of the gob, the rate of flow will also be specified. That is, if the type of glass, temperature (viscosity), shearing frequency and flow rate are controlled at the feeding machine orifice, then the desired gob will be produced. Thus the parameters to be controlled in the tube are outlet temperature (viscosity) and flow rate. If one considers the glass to have a resistance (impedance) to fluid flow then by maintaining a given level of glass in the mixing section and by maintaining this fluid impedance across the tube (inlet to outlet), then the flow will be controlled. This

impedance is related to the viscosity (temperature) distribution in the tube. Traditionally the axial temperature gradient is maintained approximately constant from the inlet to the outlet of the downcomer. In this case, the outlet temperature, the axial distribution and the inlet temperature are completely specified as soon as the desired outlet viscosity and the flow rate are fixed. Thus this system has a single operating point. This in turn will specify the outlet and inlet temperatures of the mixing section, and thus the outlet temperature of the conditioning section.

The initial state of the glass entering the forehearth is fixed within limits by the melting and fining process in the glass furnace. The final state has been established by working back from the required condition at the feeding machine orifice. Now the control effort in the cooling and conditioning sections is to regulate the state of a parcel of glass as it moves from the entrance of the forehearth to the stirring device.

Consider the downcomer as a subsystem of the overall glass process. The inputs are the temperature of the inlet glass, the heat added by the electrical heaters, the environment (or ambient temperature) and the level of the glass in the stirring section. The outputs are the temperature (viscosity) distribution of the glass and the flow rate. The process under consideration can be depicted as follows:

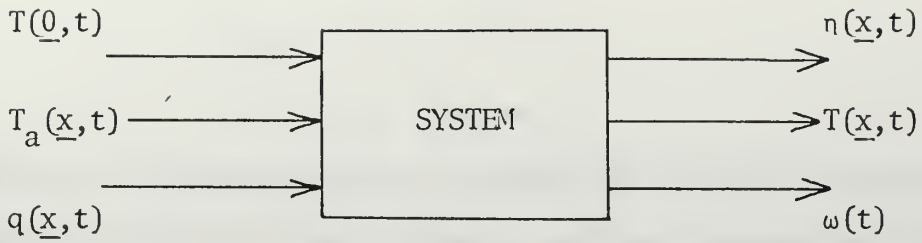


FIGURE 5-3

where

$T(0,t)$ is the inlet temperature (temperature of the glass in the mixing area)

$T_a(x,t)$ is the ambient temperature (temperature adjacent to the insulation)

$q(x,t)$ is the heat added by electrical heaters

$\eta(x,t)$ is the viscosity of the glass

$T(x,t)$ is the temperature of the glass in the tube

$\omega(t)$ is the flow rate

The temperature distribution can be considered as the "operating point". In order to expand from a single mode of operation to an operating space, one must consider the origin of the specifications on the downcomer subsystem. There is a performance index (expressed in terms of the system parameters) for the overall glass process. Let this be denoted as:

$$P = P \text{ (system parameters)}$$

Now in order to maximize performance, each subsystem must operate at a desired operating point. For the downcomer subsystem, the outlet temperature and the flow rate must be regulated. This will result in two load constraints on this system, namely:

$$T_{out} = T_{out\ desired}$$

$$\omega = \omega_{desired}$$

These load constraints can be satisfied by an infinite number of temperature distributions. However, only one temperature distribution has a constant linear gradient from inlet to outlet. One can show that the "volumetric average viscosity" of the glass in the downcomer is inversely proportional to the flow rate. Therefore one need only insure that this volumetric average is regulated at a constant that is determined by the desired flow rate. This is equivalent to regulating the fluid impedance of this fluid. Thus by not imposing the constant temperature gradient requirement, there will be an infinite number of acceptable temperature distributions (operating points). To achieve approximately a linear temperature gradient and yet allow some flexibility, one can minimize the deviation from a desired linear gradient, and still insure that the load constraints are satisfied. Before the linear gradient requirement was relaxed, the operating constraints on this system need not be expressed because they were redundant. Now one must analyse this system for operating constraints. The events that can jeopardize the operation of this system are the loss of one or more of the heaters and/or the loss of control for this process. For example, if the power level of any one of the control heaters approaches zero, the flow and temperature control will be lost, resulting in a poorer quality glass and a reduction in profits.

Thus one operating constraint will be

$$0 \leq \delta_i \leq q_i$$

where q_i is the heat added by the electrical heaters for the I-th section. Similarly, there are operating constraints restricting power to below some maximum value.

$$q_i \leq \beta_i$$

This constraint insures that the heater is not lost due to the action of an automatic protection device during normal operation. In order to be useful, the operating and load constraints must be expressed in terms of the variables of the operating space (the temperature distribution). In the next chapter this system (the downcomer) will be developed in more detail to illustrate actual implementation of contingency control. To accomplish this, disruptive disturbances that will cause constraint violations need to be enumerated. Then corresponding to each of these contingencies, security constraints must be developed. Then the operating point can be selected so as to be secure with respect to these contingencies. If one considers this as a dynamic problem, then the security constraints will be relaxed and imposed to achieve the desired degree of security. However, the optimization will strive to achieve an operating point that is as close as possible to the desired operating point. In this manner the trade-off between security and performance can be handled as a dynamically constrained optimization problem.

Before continuing on this implementation, consider one other application to the glass manufacturing process. This example occurs in the stirring area. At high viscosities, the torques required of the motor that drives the stirring mechanism can become excessive. For optimal performance in stirring the glass, it is desirable that the speed of the stirrer be maximized. Yet the torque on the motor is proportional to the stirring speed times the viscosity of the glass. As the torque increases, either the drive motor will be damaged or the stirring mechanism will break. Either of these events will bring the production line to a standstill, resulting in a large financial loss in addition to the cost of repairing the damage and restarting the process. The contingency is an unexpected increase in glass viscosity. Traditionally this stirrer is operated at a maximum speed and this is maintained constant once the process has been started. There is a single operating constraint and no load constraints on this system. The operating constraint states that the stirrer speed times the viscosity must be less than some safe value. There are two security control approaches. One can implement a form of on-line contingency control. By measuring viscosity (or temperature) and then continuously maximizing the stirrer speed subject to the operating constraing, the system will be secure. As the viscosity increases the speed will automatically be reduced. As a result of reducing the stirring speed, the efficiency of the stirrer will go down. This may be reflected by an

increase in the number of rejected pieces of glassware. However this small increase in the amount of cullet is less costly than shutting down the entire process. If there is a lag in the measurement, then an alternative approach is to create a security constraint that is more conservative than the operating constraint. If for example, one wants to be secure with respect to an unexpected increase in viscosity of $\Delta\eta_I$, then for the operating constraint

$$\eta \cdot N \leq K$$

The security constraint is:

$$\eta \cdot N + \Delta\eta_I \cdot N \leq K$$

where

N is the stirrer speed

η is the measured viscosity

$\Delta\eta_I$ is the contingency

K is a (safe constant)

This stirrer will be operated at a speed of

$$N(\eta) = K/(\eta + \Delta\eta_I)$$

This example is extremely simple yet it demonstrates the concepts of contingency control for a one-dimensional operating space. It also demonstrates the fact that the security constraints can coincide with the operating constraints. This was the case when the viscosity was being measured continuously, or when $\Delta\eta_I = 0$.

There are other simpler solutions to this problem, such as the installation of slip clutches or circuit breakers to provide automatic protection. However, this example was presented to illustrate the formulation of security constraints for the simplest possible case, i.e., a one-dimensional operating space.

In these three examples, in order to insure security it was necessary to impose security constraints. If one were to decide that the system must always be secure with respect to these contingencies then the security constraint might be added to the other constraints on a permanent basis. However, if it need only be imposed under certain conditions, then provision can be made to relax and impose the security constraint in order to affect a trade-off between security and performance. It must be recognized that when the constraint is relaxed and the contingency occurs that there will be a penalty, damage and/or a financial loss.

In the electrical power example, if the contingency occurred and the constraint had been imposed, no additional damage or financial loss would be experienced. This was also true in both glass examples. In the stirrer example, the selection of a security constraint that involved both a term representing performance (stirrer speed) and a term that was related to the contingency (viscosity) allowed a trade-off to be realized in a straightforward manner. In general, this will not be the case. The trade-off between security and performance will not be a simple relationship.

CHAPTER VI

IMPLEMENTATION OF CONTINGENCY CONTROL

In the last chapter, a portion of the glass manufacturing process was described in detail. That portion was the downcomer subsystem. It was used to demonstrate how an operating space can be created from a single operating point. In this chapter, it will be used to demonstrate the implementation of contingency control.

The Downcomer Subsystem

This part of the glass process can be briefly described as follows: glass from the forehearth conditioning section enters a mixing area. After being mixed, it flows through a platinum tube (the downcomer) to a shearing device. The outlet temperature and the flow rate are being regulated by controlling the heat being lost to the environment. This control is being accomplished by six sections of electrical heaters which regulate the axial temperature distribution. Since the shearing device does not regulate flow but merely interrupts a continuous stream of molten glass to produce gobs of the correct size, then the shearing device can be considered external to this system. Thus the system under consideration is a viscous fluid flowing through a heated metal tube. The following assumptions were necessary. The inlet fluid was considered to be homogeneous and the distribution of heat added was considered to

be piecewise constant. The fluid motion results from a driving force, namely the static head developed by the gravitational force on this fluid. To fully understand this system it is necessary to develop and study a realistic mathematical model.

The Mathematical Model

This system involves both heat and mass transfer. By considering a differential element and applying Newton's law of motion, the equations of motion were developed. The development paralleled that given by Long (22). For glass, the only body force of importance is the gravitational force. If one assumes a linear relationship between the dynamic stress and the rate of strain and also that the glass is isotropic, then the resulting equations will be the classical equations of a Newtonian fluid.

$$\rho dV D^2 x_i = \rho G_i dV + \sum_j \frac{\partial S_{ji}}{\partial x_j} dV$$

where

$$S_{ji} = -p\delta_{ji} + \lambda\sigma\delta_{ji} + 2\mu\varepsilon_{ji}$$

ρ = density of the glass

dV = the incremental volume

G_i = the I-th component of the gravitational force

S_{ji} = the I-th component of the stress force per unit area exerted across the surface normal to the

j-th axis on the material pierced by the minus j-th axis

δ_{ji} = the Kronecker delta

ε_{ji} = the rate of strain tensor = $1/2 \left(\frac{\partial v_i}{\partial x_j} + \frac{\partial v_j}{\partial x_i} \right)$

v_i = the I-th velocity component

μ = the dynamic coefficient of viscosity

σ = the divergence of the velocity = $\sum_i \frac{\partial v_i}{\partial x_i}$

D = the time rate of change = D/DT

For the pressures under consideration, the molten glass was considered to be incompressible. The equation resulting from the requirement that the mass within the differential element be conserved was

$$D(\rho dV) = 0$$

Using this, the equations of motion reduce to the Navier-Stokes equations for a viscous imcompressible Newtonian fluid.

By considering an energy balance on this same differential element of glass the accumulation of thermal energy can be equated to the net heat transfer into this element. The resulting differential equation is as follows:

$$\rho dV \, C_p \frac{\partial T}{\partial t} = \sum_i \frac{\partial}{\partial x_i} \left(k' \frac{\partial T}{\partial x_i} - \rho \, C_p \, T v_i \right) dV$$

where

C_p = the specific heat of the glass

T = the temperature of the glass

k' = the equivalent coefficient of thermal conductivity

The exact solution to this set of four nonlinear partial differential equations has not been found. By making additional simplifying assumptions certain steady state and one dimensional transient problems were solved and studied. These exact solutions were valuable in making engineering approximations and later simulating this system.

For example, if one assumes that the flow is laminar and fully developed, then the steady state velocity and temperature distributions can be calculated.

$$v(r) = \frac{g_c}{4\mu} \left(\frac{-dp}{dx}\right) (r_i^2 - r^2) = V_{max} \left(\frac{r_i^2 - r^2}{r_i^2}\right)$$

where

g_c = Newton's gravitational constant

p = the pressure

r_i = the internal radius of the tube

r = the distance from the centerline

The average velocity is:

$$\langle v(r) \rangle = V_{avg} = \frac{1}{A_c} \int_0^{r_i} v(r)\, dA$$

where

$$dA = 2\,\pi r\, dr$$

A_c = the cross-sectional area

From this one finds

$$V_{max} = 2 \cdot V_{avg}$$

The average velocity is known and is related to the mass flow rate:

$$V_{avg} = \omega/3600\,\rho\,A_c \quad \text{(ft./sec.)}$$

where

ω = the mass flow rate in lb/hour

ρ = the density in lb/cubic foot

The Navier-Stokes equations were used to develop the parabolic velocity distribution (Poiseuille flow). The derivation and implications of Poiseuille flow have been summarized by Bird (7). Another important result was the relationship between the flow rate and the pressure gradient.

$$-dp/dx = k_1\,\omega\mu$$

where

$$k_1 = 8 \,/\, 3600\,\rho\,A_c\,g_c\,r_i^2$$

This will be valuable in the development of the load constraints for this system.

Knowing the steady state velocity distribution, one can calculate the fully developed steady state temperature distribution.

$$T(x,r) = T(x,r_i) - \frac{2\rho C_p V_{avg} r_i^2}{k} \frac{dT}{dx} \left[\frac{3}{16} - \frac{1}{4} \left(\frac{r}{r_i} \right)^2 + \frac{1}{16} \left(\frac{r}{r_i} \right)^4 \right]$$

Assuming that the radial heat flux is constant produces some very useful results. Specifically, the steady state axial temperature gradient is a constant. Moreover, the axial temperature gradient at the wall of the metal tube, the axial temperature gradient at the centerline and the axial temperature gradient of the bulk temperature (flow-average temperature) are all equal to the same constant. This is of particular importance for it justifies the attempt to maintain a constant linear temperature gradient for the entire length of the downcomer. It also justifies the use of a one dimensional simulation of this system.

In the preceding chapter, this system was depicted as a relation between a set of inputs and a set of outputs. Now using the assumption that the heat added is piecewise constant, one can develop the system as six similar subsystems in series. These subsystems correspond to the six sections, each having its own heater for temperature control. To reduce the dimensionality of this system, consider the bulk temperature

$$T_B(x,t) = \frac{\langle v(r)\ T\ (x,r,t) \rangle}{\langle v(r) \rangle}$$

where

$$\langle v(r) \rangle = V_{avg}$$

Let

$T_{i-1}(t)$ be the inlet bulk temperature

$T_i(t)$ be the outlet bulk temperature

$\eta_i(t)$ be the average viscosity of the I-th section

$q_i(t)$ be the heat added by the electrical heaters for the I-th section

$q_{Gi}(t)$ be the net heat loss by the glass in the I-th section

$q_{Li}(t)$ be the heat loss to ambient in the I-th section

Assume that the ambient temperature adjacent to the insulation is a constant, T_a . Then each subsystem can be considered as follows:

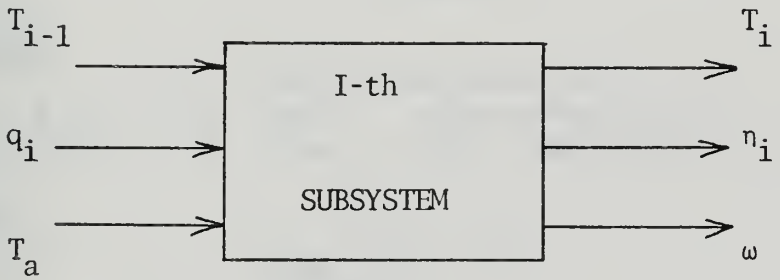


FIGURE 6-1

Note that

$$\Delta P_i / \Delta L_i = -k_1 \omega \eta$$

$$\Delta L_i = L_i - L_{i-1}$$

This subsystem can be represented by the following linear approxi-

mation,

$$T_i(s) = T_{Ti}\, T_{i-1}(s) + T_{qGi}\, q_{Gi}(s)$$

where

$T_i(s)$ is the LaPlace transform of $T_i(t)$

$T_{Ti} + T_{qGi}$ are the appropriate transfer functions

$q_{Gi}(s)$ is the LaPlace transform of $q_{Gi}(t)$

In block diagram form,

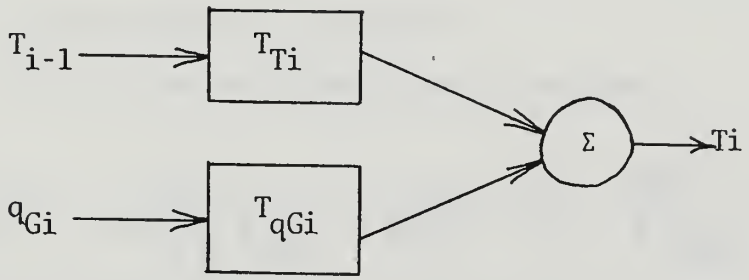


FIGURE 6-2

where

$$T_{Ti}(s) = \exp\left\{-\frac{\Delta L_i s}{V_{avg}} - \frac{\Delta L_i\, 2h\, C_1\, s}{\rho\, C_p r_i\, V_{avg}(1+C_1 s)}\right\}$$

and

$$C_1 = \frac{\rho_w C_{pw}\,(r_0^2 - r_i^2)}{2 r_i h}$$

This can be approximated by

$$T_{Ti}(s) \simeq \exp\left\{-\frac{v_i}{F}\left(1 + \frac{m_w\, C_{pw}}{\rho\, A_c C_p}\right) s\right\}$$

Gould (14) discusses the justification of this approximation.

Where

V_i is the volume of the I-th section

F is the volumetric flow rate

m_w is the mass of the pipe per unit length

C_{pw} is the specific heat of the wall

C_p is the specific heat of the glass,

ρ is the density of the glass

A_c is the cross-sectional area of the glass

$$T_{qGi}(s) = \frac{\Delta L_i}{\rho\, C_p r_i\, V_{avg}} \left(\frac{1}{1+C_1 s}\right) \exp\left\{\frac{-\Delta L_i s}{2\, V_{avg}}\right\}$$

A more sophisticated non-linear approximation was suggested by Paynter (25 and 10).

Now that the system has been described; an appropriate mathematical model has been developed; and a one-dimensional linear approximation to this model has been developed, the process can be simulated. This simulation will be necessary in the development of the control system.

Traditional Control

The traditional control is straightforward. On the direct control level, the outlet temperature of each of the six subsystems is

being regulated. The set points are determined on the basis of the performance of the downcomer and the performance of the overall glass manufacturing process. Overall performance determines the desired outlet temperature, T_{6D} , and the desired flow rate ω_D . Once T_{6D} and ω_D have been specified, then the set points, T_{is} $i = 0, 1, 2, ---, 6$, can be selected to optimize the performance of the downcomer. There are several alternate measures of downcomer performance. For example, one can minimize the electrical heater power. This can be expressed as:

$$\min \underline{C}^T \underline{q}$$

Since

$$q_{Gi} = K_{Gi} (T_{i-1} - T_i)$$

$$q_{Li} = K_{Li} (T_i + T_{i-1} - 2T_a)$$

This minimization can be expressed as:

$$\min \underline{d}^T \underline{T}_s$$

subject to

$$T_{6s} = T_{6D}$$

$$\omega(\underline{T}_s) = \omega_D$$

and

$$\underline{T}_s^T = (T_{0s}, T_{1s}, \cdots , T_{6s})$$

An alternate optimization would be to minimize the deviation from a linear gradient subject to the requirements that the desired flow

rate and the desired outlet temperature be maintained. The multi-level decomposition for a traditional control system is shown in Figure 6-3.

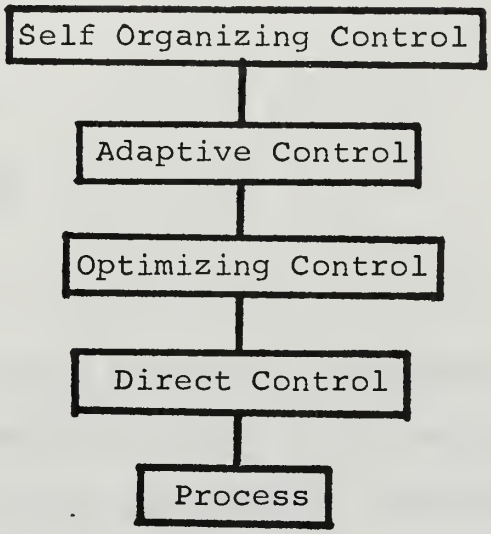


FIGURE 6-3

Previously, only direct control had been implemented on the downcomer system. Before describing the security control that is applicable to this process, the requirement that the desired flow rate be maintained needs further development.

A relationship between the flow rate and the axial pressure gradient for steady state fully developed laminar flow in a tube was previously given as:

$$-dp/dx = k_1 \omega \eta$$

For each section this equation becomes

$$\Delta p_i = - k_1 \omega \eta_i \Delta L_i$$

But for the entire downcomer,

$$\rho g h + \sum_i \Delta P_i = 0$$

or

$$\rho gh = k_1 \omega \sum_i \eta_i \Delta L_i$$

For the case where

$$\Delta L_i = \text{constant; for all } i$$

$$\rho gh = k_2 \omega \sum_i \eta_i$$

Security Control

The security control problem is a constrained optimization problem where the constraints result from load requirements, operating requirements and security requirements. Both optimization problems (described in the previous chapter) were considered. The minimization of heater power was quite simple and did not really resemble the actual operation of this process. Minimizing the deviation from a linear gradient closely approximates how the process is actually operated. If one attempts a leasts squares fit to the linear gradient, the optimization problem becomes a quadratic programming problem. Using Wolfe's technique this quadratic programming problem can be reduced to a special type of linear programming problem. This approach was taken and was found to be rather complex and time consuming when one tries to relax and impose security constraints. Finally, a curve fitting approach (Kelley's (19)) was used to minimize the maximum deviation from a desired curve. Originally the operating space was composed of an infinite

number of temperature distributions. By considering the heat added to be piecewise constant, this infinite dimensional operating space can be replaced by a seven dimensional operating space. Each vector consists of seven temperatures, taken at specified intervals along the platinum tube.

$$\underline{T}^T = (T_0, T_1, \cdots, T_6)$$

T_0 is the bulk inlet temperature and T_6 is the bulk outlet temperature. If T_{iD} is the desired bulk temperature out of the I-th section (found by solving a linear algebra problem), then the deviation d_i, is:

$$\underline{T}_S - \underline{T}_D = \underline{d}$$

In this particular implementation, a linear program was used to solve the constrained optimization. Therefore the unrestricted seven dimensional varible $\underline{d}$ was considered to be composed of two non-negative variables.

$$\underline{d} = \underline{d}' - \underline{d}''$$

In order to minimize the maximum deviation from the gradient another variable was necessary, namely the maximum deviation, D. Using these twenty-two variables, the optimization without operating, load or security constraints becomes

$$\min D$$

Subject to: $\underline{T}_S - \underline{d}' + \underline{d}'' = \underline{T}_D$

$\underline{d}' - \underline{1}\, D \leq 0$

$\underline{d}'' - \underline{1}\, D \leq 0$

The load constraints are a result of the performance of the overall glass process. The load constraints are

$$T_{6S} = T_{6D}$$

and

$$\sum_i \eta_i(\underline{T}_S) = \frac{\rho g h}{K_2 \omega_D}$$

The first load constraint will fix T_{6S} and will be satisfied by any continuous temperature distribution that begins with T_0 and ends with T_{6D}. The second load constraint requires that the average viscosity be a constant. This constant is determined by the desired flow rate.

In order to operate this subsystem properly it is desirable that the heater power be maintained within certain limits. For example, if the power level of any one of the control heaters approaches zero, the flow and termperature control will be lost, resulting in a poorer quality glass and a reduction in profits. Thus one operating constraint will be

$$0 \leq \delta_i \leq q_i$$

This becomes

$$\delta_i + 2K_{Li}\, T_a \leq (K_{Li}+K_{Gi})\, T_i + (K_{Li}-K_{Gi})\, T_{i-1}$$

In a similar manner, there are operating constraints restricting power to below some maximum value

$$q_i \leq \beta_i$$

This constraint insures that the heater is not lost due to the action of an automatic protection device during normal operation. It becomes

$$(K_{Li}+K_{Gi})T_i + (K_{Li}-K_{Gi})\ T_{i-1} \leq \beta_i + 2K_{Li}T_a$$

The third type of operating constraint may result from a restriction on the sum of the heater powers.

$$\sum_i q_i \leq \gamma$$

In order to be useful in this linear program, each of these load and operating constraints must be converted into the form

$$\underline{a}_j^T \underline{T}_S \ \Delta\ b_j$$

where Δ can be $\leq, =$ or $\geq$. For this system, this was accomplished and the collection of operating and load constraints was expressed as:

$$A_0 \underline{T}_S \ \Delta\ \underline{b}$$

In order to illustrate the development of security constraints, two contingencies will be analyzed. These are by no means the only contingencies pertinent to this example. The first contingency will result in a single violation of one of the load constraints. The

second will result in violations of both operating and load constraints. The two to be considered are (1) a change in glass level in the forehearth and mixing areas and (2) a change in the inlet temperature. A large change in forehearth level can be due to material being fed into the glass furnace either too fast or too slowly (due perhaps to a faulty auger drive mechanism). A large change in downcomer inlet temperature can be due to a failure of the forehearth temperature control or the securing of gas to the flaming jets that heat the glass in the forehearth. Without analysing the cause consider the effect on the downcomer subsystem.

Any change in either the glass level or the inlet temperature will result in a violation of the operating or load constraints. This can be demonstrated with the process simulation or by considering that

$$\omega = \rho g h / k_2 \sum_i \eta_i$$

Any increase or decrease in level will result immediately in a change in flow rate. After an appropriate time delay, the outlet temperature increases (decreases) for an increase (decrease) in inlet temperature. In each section, as soon as the change in outlet temperature occurs the controllers react, however there is a lag before the effect of the controller is realized. Thus this system still can not be made secure with respect to certain contingencies. This demonstrates an important point; if a contingency will result in

the violation of an equality constraint (load or operating), there does not exist a security constraint that will insure security with respect to this contingency. Therefore the load constraints on this system must be considered more closely.

In reality, there are usually tolerances on the system parameters. That is, these system parameters may be allowed to vary as follows:

$$\omega_{min} \leq \omega \leq \omega_{max}$$

$$T_{6min} \leq T_6 \leq T_{6max}$$

without any measurable degradation of overall system performance, or with some acceptable reduction. If this is the case, then the rigid load constraints can be relaxed. For example, if

$$\underline{a}_\kappa^T \underline{T}_S = b_\kappa$$

is equivalent to

$$\sum_i \eta_i(\underline{T}_S) = \rho g h / k_2 \omega_D$$

in the linear program, then it can be replaced by:

$$\underline{a}_\kappa^T \underline{T}_S \leq b'_\kappa$$

$$\underline{a}_\kappa^T \underline{T}_S \geq b''_\kappa$$

$$\underline{a}_\kappa^T \underline{T}_S - d'_8 + d''_8 = b_\kappa$$

$$d'_8 - D \leq 0$$

$$d''_8 - D \leq 0$$

and $T_{6S} = T_{6D}$

replaced by:

$$T_{6S} \lesssim T_{6max}$$

$$T_{6S} \gtrsim T_{6min}$$

$$T_{6S} - d_7' + d_7'' = T_{6D}$$

$$d_7' - D \lesssim 0$$

$$d_7'' - D \lesssim 0$$

In the actual implementation, tolerances on the outlet viscosity were used to generate the maximum and the minimum values for the outlet temperature. The system simulation was used to find the corresponding tolerances on the other temperature set points. Now the system can be operated in such a manner to be secure with respect to either an increase or a decrease (but not both) of

$$\Delta h_s = \frac{k_2(\omega_{max}-\omega_{min}) \sum_i \eta_i}{\rho g}$$

It can be operated so it is simultaneously secure for either an increase or a decrease of $\Delta h_s/2$. This illustrates an important point, that the increasing and the decreasing levels are separate contingencies and should be treated as such.

First consider an increase in level. The maximum increase for which the system can be made secure is Δh_s and for any $\Delta h_I \lesssim \Delta h_s$ the security constraint to insure that the system is secure with

respect to Δh_I is:

$$\omega \leq \omega_{max} - \frac{\rho g \, \Delta h_I}{k_2 \sum_i \eta_i}$$

Similarly for a decrease Δh_D , where

$$\Delta h_D \leq \Delta h_s$$

there is a security constraint of

$$\omega \geq \omega_{min} + \frac{\rho g \, \Delta h_D}{k_2 \sum_i \eta_i}$$

. In this case if

$$\Delta h_I + \Delta h_D > \Delta h_s$$

then the system can not be secure with respect to both contingencies.

In other problems it may not appear as straightforward as this example but in essence ω is indirectly an element of the operating space and the distance from one extreme of the normal portion of this operating space to another extreme expressed in terms of ω is $\omega_{max} - \omega_{min}$. This distance must be mapped into the contingency space, of which level is just one element. The corresponding distance is Δh_s , and this is the maximum change of h for which this system can be secure without redefinition of the boundary of the normal operating space. Note that there may be a penalty for imposing the security constraint. Namely, if

$$\omega \neq \omega_D$$

then

$$P(\omega, T_{6D}) \leq P(\omega_D, T_{6D})$$

and the penalty is the difference

$$P(\omega_D, T_{6D}) - P(\omega, T_{6D})$$

Now consider the more complicated contingency, a radical change in the bulk inlet temperature. Again this should be separated into two distinct contingencies, the increase and the decrease. First consider an increase in inlet temperature. There are several effects of this contingency. It will cause

$$T_6 > T_{6D}$$

thus violating a load constraint. The other temperatures, T_i , along the downcomer will increase causing the viscosities to decrease. The average viscosity will not be equal to the desired constant and the flow rate will increase.

$$\omega > \omega_D$$

Since the increasing inlet temperature will result in a decrease in the power required by the electrical heaters, one of the heaters may approach its lower limit.

Can the system be made secure with respect to this contingency? As mentioned before, there are tolerances on ω and T_6 .

$$\omega_{min} \leq \omega \leq \omega_{max}$$

$$T_{6min} \leq T_6 \leq T_{6max}$$

Using either the inverse system relations or the simulation one can find out how the distances $T_{6max} - T_{6min}$ and $\omega_{max} - \omega_{min}$ map onto the contingency space. Let the corresponding ranges in inlet temperature be ΔT_{0T} and $\Delta T_{0\omega}$. That is ΔT_{0T} is the maximum change in inlet temperature the system can suffer without violating the load constraint on the outlet temperature and $\Delta T_{0\omega}$ is the maximum change in inlet temperature that will not cause a violation of the load constraint on flow rate. The system can be made secure only with respect to the smaller change. Before determining this value, the change in inlet temperature which will cause a violation of a heater constraint must also be calculated. Let these be denoted as ΔT_{0i}, I = 1,2,---,6. The distances in the operating space are:

$$\beta_i - \delta_i$$

Now

$$\Delta T_{0s} = \min \{\Delta T_{0i}\} \; i = 1,---,6,T,\omega$$

where ΔT_{0s} is the maximum increment for which the system can be made secure. Suppose one would like to be secure with respect to both an increase of ΔT_{0I} or a decrease of ΔT_{0D}, where

$$\Delta T_{0I} + \Delta T_{0D} \leq \Delta T_{0s}$$

then the security constraints will be

$$\delta_i + \frac{(\beta_i - \delta_i)}{\Delta T_{0i}} \Delta T_{0D} \leq q_i \leq \beta_i - \frac{(\beta_i - \delta_i)}{\Delta T_{0i}} \Delta T_{0I}$$

$$T_{6min} + \frac{(T_{6max} - T_{6min})}{\Delta T_{0T}} \Delta T_{0D} \leq T_6 \leq T_{6max} - \frac{(T_{6max} - T_{6min})}{\Delta T_{0T}} \Delta T_{0I}$$

$$\omega_{min} + \frac{(\omega_{max} - \omega_{min})}{\Delta T_{0\omega}} \Delta T_{0D} \leq \omega \leq \omega_{max} - \frac{(\omega_{max} - \omega_{min})}{\Delta T_{0\omega}} \Delta T_{0I}$$

For this example, one can see that the system can be made secure for any increase

$$\Delta T_{0I} \leq \Delta T_{0s}$$

or any decrease

$$\Delta T_{0D} \leq \Delta T_{0s}$$

and simultaneously secure for either, if

$$\Delta T_{0I} + \Delta T_{0D} \leq \Delta T_{0s}$$

Now that the security constraints have been formulated for the contingencies Δh_I , Δh_D , ΔT_{0I} and ΔT_{0D} , the corresponding constraints can be added to the optimization if one wants to be secure with respect to one of these contingencies. This implementation of contingency control was carried out to the following extent. The process was not available for manipulation and study. Therefore,

a simulation of the process was developed. It was simulated in six sections corresponding to the six heaters and their areas of direct influence. Six PID controllers were simulated, added to the process simulation and tuned. These direct controllers responded to errors between the sectional outlet temperatures and the temperature set points. Optimizations to generate these set points where developed for three cases without security control and then for the same three cases with security control. These cases were: the minimization of heater power, the achievement of a linear gradient based only on a desired outlet temperature and flow rate, and the minimization of a maximum deviation from a desired flow rate and temperature distribution. Security control could not be applied to the second case because the operating space consisted of a single operating point. The third optimization was the most realistic of the three and closely approximated the operation of the actual system. The linear programming problem that was used to minimize the maximum deviation from a desired flow rate and temperature distribution contained fifty two constraints, as follows:

8 equality constraints

30 inequality constraints

14 upper and lower bounds

Ideally, one would like to close the loop between the system and the security controller by calculating the EMV dynamically as a function of the present operating point. Sufficient plant

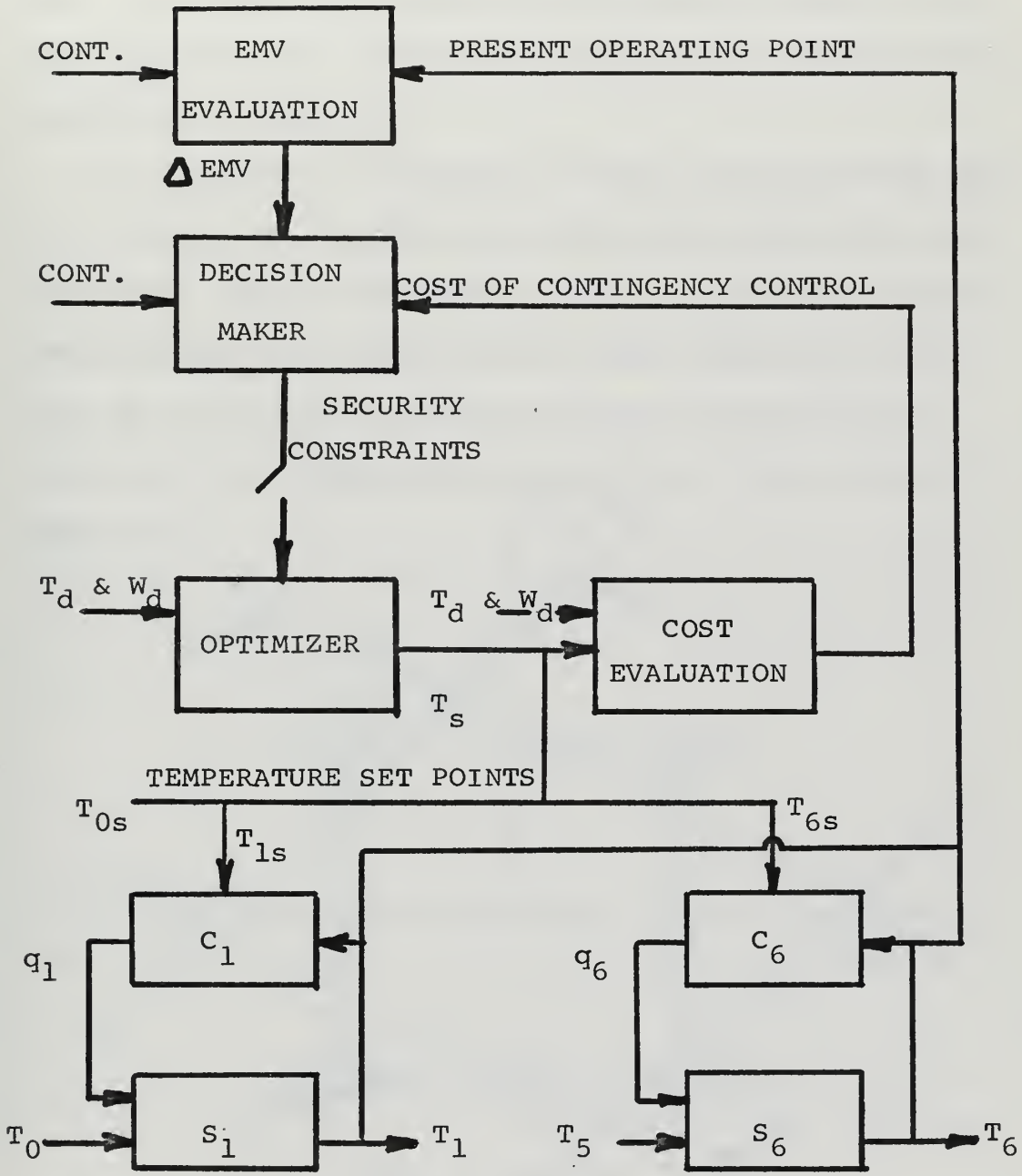

CONT.
EMV EVALUATION
PRESENT OPERATING POINT
Δ EMV
CONT.
DECISION MAKER
COST OF CONTINGENCY CONTROL
SECURITY CONSTRAINTS
T_d & W_d
OPTIMIZER
T_d & W_d
COST EVALUATION
T_s
TEMPERATURE SET POINTS
T_{0s}
T_{1s}
T_{6s}
C_1
C_6
q_1
q_6
S_1
S_6
T_0
T_1
T_5
T_6

FIGURE 6-4

operating data was not made available to accomplish this. The performance function for the overall glass process was assumed to be known. In an actual implementation, these would be known and the loop could be closed. The overall implementation is shown in block diagram form in Figure 6-4.

It is impossible to illustrate the entire normal operating space as it actually was, because it was a twenty-four dimensional operating space. However by considering only one section and using the deviations from the desired input and output temperatures as the axis, one can project all of the constraints that affect this section onto a two dimensional representation. This is shown in Figure 6-5.

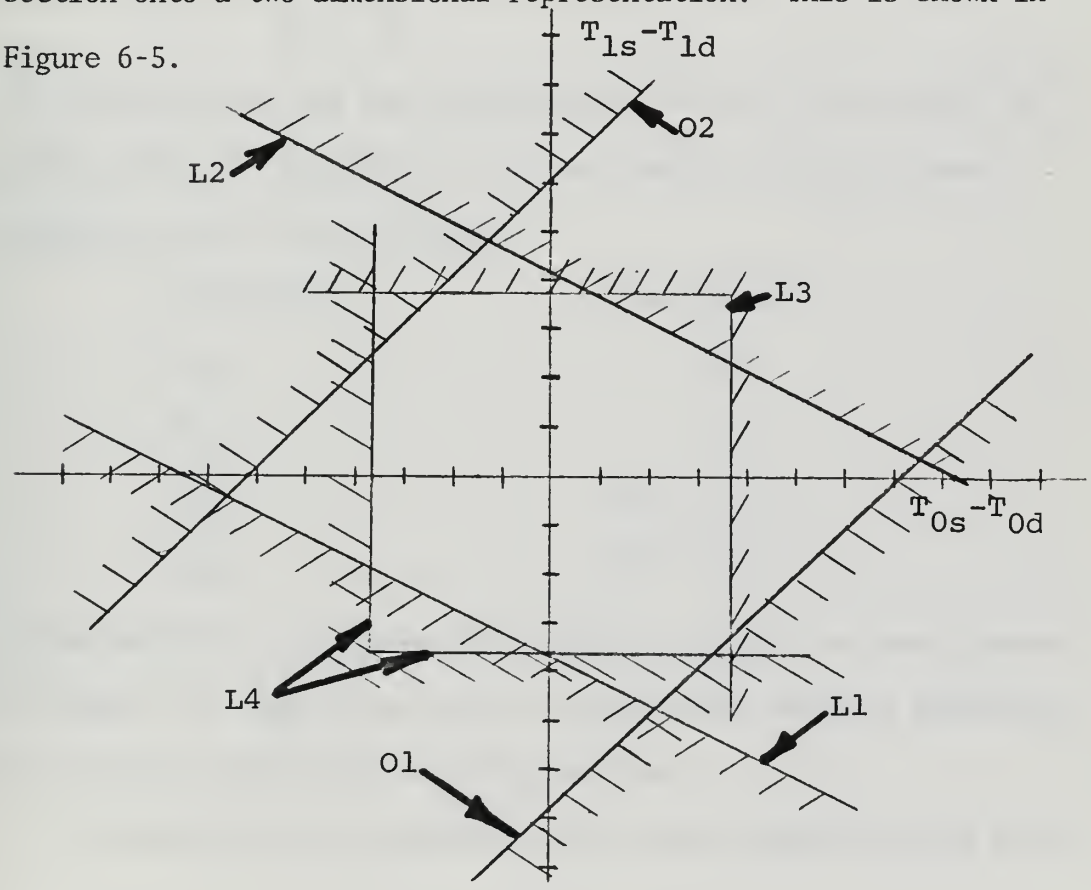


FIGURE 6-5

This is the operating space as it would be if all other sections were operating at their desired operating points. The constraints are numbered. They correspond to the following load and operating constraints:

L1	ω	$\geq \omega_{min}$
L2	ω	$\leq \omega_{max}$
L3	η_6	$\geq \eta_{6min}$
L4	η_6	$\leq \eta_{6max}$
01	q_i	$\geq \delta_i$
02	q_i	$\leq \beta_i$

The contingencies and the constraints which they can violate (depending upon the magnitude of the contingency and the present operating point) are as follows:

Contingency	Constraints
Δh_I	L2
Δh_D	L1
ΔT_{0I}	01, L2, L3
ΔT_{0D}	02, L1, L4

If one envisions the appropriate security constraints superimposed on Figure 6-4, then it is easy to see how they restrict operation to a secure region of this operating space.

In conclusion, the implementation of contingency control to the

glass manufacturing process was a linear programming problem that consisted of a minimization of the maximum deviation from a set of desired system parameters. This minimization was subject to system constraints, load constraints, operating constraints, and security constraints. The system constraints related the desired system parameters to the variables of the operating space. The operating and load constraints established the boundary of the normal operating space. The security constraints moved the operating and load constraints in order to insure security with respect to a given contingency. The imposition of security constraints changed only the requirements vector in the linear programming problem. The decision as to whether or not to change an element or a set of elements of the requirements vector in order to secure was made as described in chapter three. For each contingency, the optimization was solved with the new requirements vector. This would result in a temperature distribution, which was used to calculate the viscosity distribution and the resultant flow rate. These can be used to calculate the reduction in the overall system performance (or the cost of being secure with respect to this contingency). This cost can then be compared with the expected improvement in the EMV of the damage due to this contingency.

CHAPTER VII

SUMMARY AND EXTENSIONS

Summary

In this dissertation, a number of things were developed.

1) Numerous previously unrelated ideas about system security were developed into a consolidated set of concepts.

2) These concepts led to the development of security control actions, that could compensate for disruptive disturbances (contingencies).

3) The concepts which were presented serve as the framework for a new type of control that involves dynamic decision-making, security and performance. With the advent of security control, computers will be able to assist in a dynamic decision making process that is presently performed by human operators and process supervisors.

4) A measure of security that depends on the present operating point was presented. This measure was used to decide implementation or non-implementation of security control actions.

5) The cost of security control actions was discussed in order to develop the guidelines for justifying security control.

6) Several examples were presented to demonstrate not only applicability but details of implementation.

7) These examples were used to demonstrate the origin of security constraints.

8) One example was developed in sufficient detail to demonstrate

the implementation aspects of contingency control.

9) An operating space was used throughout the thesis instead of relating to a state space. This emphasizes the use of variables which are already available for the operation and control of a system.

10) The partitioning of the operating space by imposing security constraints was demonstrated in the downcomer example.

11) The use of a linear program for the constrained optimization had several advantages. It was a simple and straightforward implementation. Security decisions could be made based on all of the operating variables. Operators tend to concentrate their attention on one or two variables which they hope are the most significant variables. The enumeration problem was relatively simple, since only the requirements vector of the linear programming problem changed.

12) The downcomer example demonstrated that processes which are presently over constrained can be operated in such a manner to take advantage of the tradeoff between security and performance. This was accomplished by creating an operating space. Then a constrained optimization problem selected the best operating point based on performance and security. The constraints were directly related to the set of next contingencies. This set was considered fixed, however it could have been dynamic without any additional complexity. The dynamic case required only that the expected monetary value be

expressed as a function of the present operating point.

Extensions

It is hoped that the immediate extensions of this research will be in the area of application. The application of security control leads to a better understanding of the overall system being controlled. It can lead to the design of better prevention and protection systems. Hopefully in some systems, it will result in an on-line implementation of contingency control. In every case where security control is to be carefully applied, the long term cost of operating the system will be less.

In addition, research efforts on security control need to continue. For example, a computer assisted implementation of contingency planning could be developed. The diagnostic portion of a contingency plan can certainly be computerized in order to achieve a quick reliable diagnosis of an emergency for a complex system. It may be possible to use the same constrained optimization developed for contingency control to generate various strategies for contingency plans on a given system. The development of a greater understanding of related sequential events (the theory of discrete events) will assist in the design of better systems for contingency prevention.

As far as systems theory and the theory of control is concerned, security control has its own natural decomposition and each section of the security controller can interact with the various levels of

multi-level control. In fact in relation to systems theory, this is an example of a multi-strata control system. The traditional control with its multi-level decomposition is in the lower stratum. The security control is in the other stratum with an entirely different decomposition. This is shown in Figure 7-1.

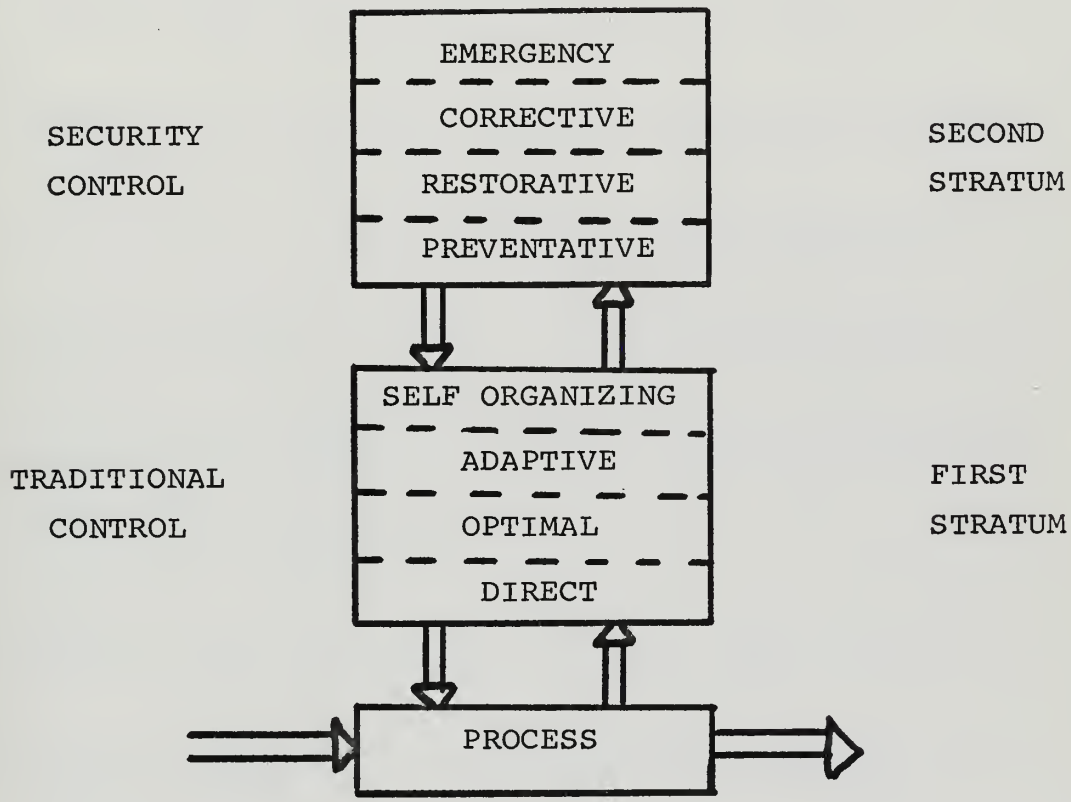


FIGURE 7-1

There is no special sequence necessary in order to develop these two strata. One can easily display examples where one has been developed first and the other later or not at all. In other cases, it might have been necessary to develop them concurrently even though neither strata is completely developed. However, with the help of the set of concepts presented in this thesis, both strata can now be developed to a greater extent.

REFERENCES

1. Angus-Butterworth, L. M. The Manufacture of Glass. New York: Pitman Publishing Corp., 1948.

2. Arkadov, A. G. and Braverman, E. M. Computers and Pattern Recognition. Washington: Thompson Book Co., 1967.

3. Arpaci, V. S. and Clark, J. A. "Dynamic Response of Heat Exchangers Having Internal Heat Sources - Part II." ASME Transactions, Vol. 80, April, 1958.

4. Arpaci, V. S. and Clark, J. A. "Dynamic Response of Heat Exahangers Having Internal Heat Sources - Part III." Journal of Heat Transfer, ASME Transactions, Series C, Vol. 81, November 1959.

5. Bardrof, F. E. "20 Years of Progress in Glass Plant Materials Handling," Glass Industry. Vol. 21, April, 1940.

6. Berlye, Milton K. The Encylclopedia of Working with Glass. Dobbs Ferry, N. Y.: Oceana Publications Inc., 1968.

7. Bird, R. Byron; Stewart, Warren E.; and Lightfoot, Edwin N. Transport Phenomena. New York: John Wiley & Sons, 1960.

8. Braverman, D. "Theory of Pattern Recognition," in Advances in Communications Systems, Vol. 1, New York: Academic Press, 1965.

9. Charan, Rama. Handbook of Glass Technology. Benares: Banaras Hindu University Press, 1956.

10. Clark, J. A.; Arpaci, V. S.; and Treadwell, K. M. "Dynamic Response of Heat Exchangers Having Internal Heat Sources - Part I." ASME Transactions, Vol. 80, April 1958.

11. Duffin, J. and Johnson K. "Glass-Container Process: Forehearth Simulation." International Business Machines Corporation Report, July 1965.

12. Dy-Liacco, Tomas E. "Control of Power Systems via the Multi-Level Concept," Ph.D. Thesis, Case Western Reserve University, June 1968.

13. Fulcher, G. S. "Analysis of Recent Measurements of the Viscosity of Glasses." Journal of American Ceramic Society, Vol. 8, 1925.

14. Gould, Leonard A. Chemical Process Control; Theory and Applications. Reading, Massachusetts: Addison-Wesley Co., 1969.

15. Hadley, G. Linear Programming. Reading, Massachusetts: Addison-Wesley Publishing Co., 1962.

16. Hammond, J. W. 20 Years of Progress in Glass Melting," Glass Industry. Vol. 21, April, 1940.

17. Hodkin, F. W. and Cousen, A. A Textbook of Glass Technology. London: Constable & Comp. Ltd., 1925.

18. Jakob, Max. Heat Transfer Vol. 1, New York: John Wiley & Sons, 1949.

19. Kelley, James E., Jr. "An Application of Linear Programming to Curve Fitting," J. Soc. Indust. Appl. Math., Vol. 6, No. 1, March 1958.

20. Lefkowitz, I. 'Multi-Level Approach Applied to Control System Design," ASME Transactions, Vol. 88, Series B, June 1966.

21. Littleton, J. T. and Morey, G. W. The Electrical Properties of Glass. New York: John Wiley & Sons Inc., 1933.

22. Long, Robert R. Mechanics of Solids and Fluids, Englewood Cliffs, N. J.: Prentice-Hall, 1961.

23. Morey, G. W. The Properties of Glass. New York: Reinhold Publishing Corp., 1938.

24. Nilsson, N. J. Learning Machines. New York: McGraw Hill, 1965.

25. Paynter, H. M. and Takahashi, Yasundo. "A New Method of Evaluating Dynamic Response of Counterflow and Parallel-Flow Heat Exchangers," ASME Transactions, Vol. 78, May 1956.

26. Perry, Josephine. The Glass Industry. New York: Longmans, Green and Company, 1945.

27. Phillips, C. J. Glass: The Miracle Maker. New York: Pitman Publishing Corp., 1941.

28. Prandtl, Ludwig. Essentials of Fluid Dynamics. New York: Hafner Publishing Co., 1952.

29. Pratt, John W.: Raiffa, Howard; and Schlaifer, Robert. Introduction to Statistical Decision Theory. New York: McGraw Hill, 1965.

30. Raiffa, Howard and Schlaifer, Robert. Applied Statistical Decision Theory. Clinton, Mass.: The Colonial Press, 1961.

31. Rogers, Frances and Beard, Alice. 5000 Years of Glass. Philadelphia: J. B. Lippincott, 1958.

32. Scholes, Samuel R. Modern Glass Practice. Chicago: Industrial Publications Inc., 1935.

33. Sellars, J. R.; Tribus, Myron; and Klein, J. S. "Heat Transfer to Laminar Flow in a Round Tube or Flat Conduit - The Graetz Problem Extended" ASME Transactions, Vol. 78, February 1956.

34. Shook, James A. "Numerical Simulation of Interacting Heat Transfer and Laminar, Viscous Flow." M.Sc. Thesis, Case Western Reserve University, November 1966.

35. Yang, W. J.; Clark, J. A.; and Arpaci, V. S. "Dynamic Response of Heat Exchangers Having Internal Heat Sources - Part IV." Journal of Heat Transfer, ASME Transactions, Series C, Vol. 83, August 1961.

Enclosure (2)

This dissertation is submitted in accordance with PGS Inst 5000.2C. It is to be deposited in the library at the U.S. Naval Postgraduate School for reference.

For Library: The following words can be used for cross-reference.

1. System Security
2. Systems Engineering
3. Control Engineering
4. Systems Analysis
5. Operations Research
6. Constrained Optimization
7. System Protection
8. Reliability
9. Contingency Planning
10. Contingency Prevention
11. Contingency Control

M. H. S.

Thesis 122750
S6645 Sollberger
Security of an
industrial system.