CONF-850903--10



# AUTOMATING LARGE-SCALE REACTOR SYSTEMS

R. A. Kisner
Oak Ridge National Laboratory*
Oak Ridge, Tennessee

CONF-850903--10

DE85 017156

## ABSTRACT

This paper conveys a philosophy for developing automated large-scale control systems that behave in an integrated, intelligent, flexible manner. Methods for operating large-scale systems under varying degrees of equipment degradation are discussed, and a design approach that separates the effort into phases is suggested.

## INTRODUCTION

Although much work has been done on reactor control, a new perspective is needed to stimulate us to rethink our objectives and methods. Such introspective activity is especially needed during transition periods such as the recent replacement of analog controllers with digital system implementations in control engineering.

With few exceptions the capabilities of mini- and microcomputer technology exceed previous control technologies. Real-time computer-based control, offering a higher level of intelligence, can perform high-level decision making and optimal complex-goal control as well as implement multivariate control schemes. Compared to discrete analog and relay design, these new capabilities demand a different perspective on automation and the control system's role in plant operation. In various industries microprocessor-based control systems are simply used to emulate the functions of classical analog control modules without exploiting the advantages of the new technology. This illustrates the need for expanded control concepts. This paper is intended to introduce a philosophy for the design of large-scale control systems that will guide control engineers and managers in the use of state-of-the-art technologies to develop integrated, intelligent, flexible systems.

Automation has different meanings for different groups (factory, aircraft, office, process, etc.). In a general sense, automation has come to mean the delegation of tasks to machine or computer systems, thus freeing human operators from vigilance over routine or tedious tasks. A distinction is made between process control and process automation. Process control, referring to the continuous regulation of a process, is a subset of process automation, which includes discontinuous activities such as decision making. As we will use it here, automation is the moving of operator functions into the realm of computer software.

A classification scheme for automation has been devised as a step in developing design guidance for large-scale nuclear power systems. The total operation of a process system can be separated into five components: controlling, configuring, monitoring, diagnosing, and planning. These become the base dimensions of automation.

This five-component breakdown is an expansion of earlier work [1], where the idea of analyzing plant automation was proposed to gain an insight into the operator's relationship to the machine portions of the plant. The types of automation were described as dimensions in automation space so that the degree of automation

*Operated by Martin Marietta Energy Systems, Inc., for the U.S. Department of Energy under Contract No. DE-AC05-84OR21400.

in a plant could be represented graphically as a multidimensional geometric form. The five dimensions are defined in the paragraphs following.

Process control refers to regulation activities directed at maintaining specific characteristics of a product stream or achieving specific performance of a continuous system. Stability, in the classical sense, is an objective of this dimension. Classical and modern control disciplines focus on controlling as defined here.

Configuration control refers to configuring the flow of process material or data, enabling the operation of a system, or selecting the function of a system to meet system goals. Goals of plant systems shift because of normal changes in the plant's operating mode, as in startup; because of equipment failure or other abnormal conditions; or because of equipment maintenance and repair. Unlike process control, configuration control is accomplished primarily by discrete actions.

Monitoring refers to the measurement and communication of process parameters and variables. Although one usually thinks of process measurement as being an automated function, chemical analysis in power plants is in fact a mainly manual activity carried out by technicians. In the most recent plant designs, computer systems provide data storage and busing to various control systems and to plant operators.

Diagnosing refers to the ability to detect or anticipate an anomaly, identify its cause, predict the consequences or propagation, and determine the proper response with respect to the mission of the plant. Computerization of this aspect of automation presents a challenge to the engineering community. Some aspects of diagnosis such as alarm generation are routinely automated. However, as it is currently implemented in most plants, alarm generation is accomplished by simple limit comparison. Work is in progress at many organizations to increase the intelligence of alarm diagnosis so that fewer extraneous data are presented to the operator. As far as automating the other aspects of diagnosis, the consensus indicates that artificial intelligence techniques such as automated reasoning and expert systems may resolve problems that do not easily yield to the application of a simple rule or template.

Planning refers to selection of overall goals and missions and the high-level scheduling of plant operating modes and allocation of resources to meet those goals. This aspect of automation, somewhat removed from on-line operation, encroaches on the former domain of human operators.

Proper allocation of functions among human and machine components is required for automation to achieve its full potential. Although it seems reasonable to approach the design of a large-scale system by attempting to state initially some mixture of human and machine participation, the actual choice depends primarily on the level of technology at the time of system design. After the capabilities of technology (primarily computer) have been determined, appropriate allocations can be made. This is in agreement with the procedure developed by Pulliam et al. [2] Proper allocation of control functions may require returning some control to the human to avoid fragmented tasks and to ensure that the operator's human factors structure and cognitive support are adequate and that job satisfaction is more nearly optimal.

## CONTROLLING WITH DEGRADED EQUIPMENT

Regardless of how much care and expense goes into the engineering of large-scale systems, they occasionally fail to function as designed because of component failures and environmental disturbances. (The range of possible environmental disturbances in large-scale systems is inherently greater than in small systems.) The

ability of a system to withstand a wide range of disturbances, specifically tolerance to failed components, is referred to as "fault tolerance." The property of "robustness" refers to systems whose parameters may range far from their usual values without serious degradation of performance. Fault tolerance and robustness can become indistinguishable at times; however, fault tolerance is associated with internal equipment failure, whose probabilities are known during design, while robustness is associated with the ability to recover from large variations in system parameters, including process variables exceeding design limits and other unplanned excursions.

A goal of design is to build in both fault tolerance and robustness. One approach is to duplicate equipment critical to plant operation. This physical redundancy, if affordable, could be implemented to the extent necessary to meet whatever reliability goals apply. A second means of fault tolerance can be provided by the plant control system by drawing on the five dimensions of automation to give it the reconfiguration capability necessary to accommodate anticipated failures. The extent of this capability is determined from a knowledge of plant availability requirements and cost versus benefit and safety considerations.

Intelligent control, which can achieve the system-wide fault tolerance and robustness desired, can be accomplished by providing good control for the plant under normal or nearly normal conditions as well as control that accommodates various states of equipment degradation or interconnection. This can be done by embedding a goal structure within the control system software. Thus, as operating conditions change, the control system should be capable of detecting such changes, overlaying the new goals of the plant, and adopting new strategies for meeting those goals.

Preliminary work has begun on a method for implementing condition-dependent control strategies by means of a hierarchical control system. For discussion purposes, a hierarchical structure is composed of levels or layers of control modules in which a module can link with both superordinate and subordinate modules. These links are communication pathways or pipelines. The data flow from superordinate to subordinate is referred to as "efferent;" subordinate to superordinate is "afferent" [3].

Condition-dependent control involves dividing the state space for the controlled system into three contiguous control regions: homeostatic, degraded, and uncontrollable. Associated with each region are appropriate operating goals and strategies for meeting those goals. A state vector is projected into this space of regions; the elements that compose the vector are a mixture of both continuous variables and discontinuous parameters. A discontinuous parameter can assume only discrete values. (In many cases it may be purely off-on in character, perhaps indicating the status of a pump or stop valve.) The result is a point in space that moves with the changing state of the plant. Fig. 1 illustrates the control regions for a simple system of two state variables.

These multidimensional regions are not fixed in space but rather are related to the target state (Fig. 1a, steady-state operation) or to both the target state and the pathway of transition (Fig. 1b, a system moving from initial to target state). Thus, not only is the vector moving as it follows the dynamics of the plant, but also the regions are being readjusted as specific limits change and the availability and operability of equipment change. The boundaries separating the contiguous regions are flexible; their relative positions depend on known plant conditions. Real-time calculations are required to determine continuously the shape and coverage of the regions. These calculations must be based on an a priori quantitative knowledge of the behavior of plant components, their failure modes, and the extent and range of maneuverability that the control system has over them. Creation of the regions also

must be based on identification of the immediately available capabilities of the control and protection systems.

The creation of one complete and overall state space for the entire plant would require concurrent analysis of thousands of data entries from the monitoring and data-handling system, which would require a large amount of computing power. A better approach is to decompose the system: resolve the state space into a set of spaces, each associated with a single plant subsystem. To effect coordination of the plant at higher levels within the control hierarchy, spaces would also be created to represent grouped systems. The complexity of the overall computation is then reduced by the power of separation and simplification. Some autonomy of control is given to the lower level controllers as they select the best strategy of control based on the commands received from the superordinate and on the region of control their state vector occupies. In effect, the state vectors of the lower level systems become the elements of the upper level vectors. Decisions made at the lower levels would be communicated upward to allow supervisory coordination of the entire plant.

The movement of a system's vector into the bordering region is an indication that significant changes in the plant have occurred or are beginning to occur. This denotes the need for a change in the general strategy being applied in the control of the affected system, and hence a change in the specific rules and procedures being used. This change of strategy may require not only proportional changes in set points and limits but also abrupt rerouting of process flows and other reconfigurations of systems and components.

The three control regions are discussed in greater detail in the following section. Many of the concepts and terms are adapted from studies of electrical power system stability [4] because of the similarities between control of large-scale power distribution systems and control of large-scale power generation plants.

## REGIONS OF CONTROL

### HOMEOSTATIC REGION

The goal of control within the homeostatic region is to produce the desired product of the plant system. In the absence of major equipment failure, behavior in this region tends to converge on the target state, which is the desired operating state. The target state, nominally a point, is a statistically defined region within the homeostatic region. Strategies for optimal control and adaptive control are employed when the system is situated in the homeostatic control region. As appropriate for the mode of control, various criteria may be chosen to cause minimum error, time, energy, or mechanical stress in controlling the system.

Power plants often change states because of maintenance or refueling schedules or load demand changes. To accomplish the transition from a known state to a desired state, a preferred pathway to the target is established and a corridor surrounding the transition pathway is created. Determination of the target pathway and the rates of change along it should be based on optimization; alternative pathways may offer a range of energy consumptions, power requirements, mechanical or thermal component stress, time to completion, or margins to unsafe plant conditions. Two possible approaches to forming a pathway or trajectory are (1) identify all of the "bad" places in state space and maneuver around them, or (2) identify a multidimensional channel and guide the plant through it. Such a path is shown in Fig. 1b. Real-time identification of the "best" transitions should be part of the control system's capability. Similar to the homeostatic region formed around the target state in steady-state operation, a corridor is formed that envelops the transition pathway.

Operation anywhere within the homeostatic region is considered "normal," even if the actual system state is not precisely within the statistical boundary of the target region. Such a condition could be described as off-target normal, where the control system is presumably driving the system state toward the target point.

Structural defects (minor faults in equipment or interconnections) are tolerated within the homeostatic region so long as the capability of the control system to maintain the target state has not been voided. Likewise, security defects (losses of redundancy) are tolerated in this region. Defect restoration could occur simultaneously with normal operation.

Determination of the boundaries between the three regions, not necessarily being a rigorous and precise quantitative calculation, may require some a priori engineering judgment in assessing the control system's capability under various possible operating conditions. Indeed, the prediction of plant response to control input becomes a matter of expert opinion, which must be embedded in software.

Should structural or security anomalies exceed tolerable limits, the homeostatic region must be redefined. For directly observable and consequential failures, it can be shrunk to the target state or removed entirely, thus leaving the system in a degraded state. Major equipment damage or malfunction as well as external disturbances of sufficient magnitude can drive the system out of the homeostatic region.

DEGRADED REGION

The goal of the control system with its state vector in the degraded region is efficient restoration of the faulted systems so that return to the homeostatic region may proceed in minimum time. More specifically, the control objectives of the degraded region are to (1) maintain continuous and uninterrupted (although perhaps reduced) delivery of the principal products of the system if possible; (2) prevent or minimize equipment damage; and (3) avert intervention by the plant safety and protection systems by maneuvering the system away from the envelope inscribed by the safety systems. For all control system responses, downtime can be reduced by generating proportionate control reactions to evolving situations rather than overreaction because of a lack of alternative reactions on the part of the control system. Three types of crises are possible within the degraded region, and each requires a different strategy for control.

1. Stability Crisis. This condition indicates that the controlled system has become unstable (stability must be defined for the specific system). The strategy is to maneuver the system to an intermediate safe and stable state which is near the original target state and which will continue to deliver the principal product for which the system was designed. Thus the major systems to which the degraded system is providing product can remain on-line, although at a reduced level. A collection of safe states must be identifiable based on constraining conditions such as known equipment or interconnection failures, and preferred pathways from the current state to the alternative safe states must be known. The precalculation and storage of the pathway, as in a sequence of actions, may not have to be made if the rules for determining the correct next state and the procedure for getting there can be embedded in the control system. This is the goal of the procedure prompting system under development at Hanford Engineering Development Laboratory [5].

A component-level example: A valve controller malfunction has introduced flow oscillations in a coolant stream, thus inducing temperature fluctuations elsewhere in the process subsystem. By lowering the power level to reduce the heat generated or bypassing the malfunctioning control valve through a smaller channel of flow, the subsystem would have a reduced output but would remain in a stable state.

2. Viability Crisis. This condition indicates that no stable state can be found which delivers the principal product to downstream systems. Thus, the strategy is to suspend (at least temporarily) the delivery of product until repair can be effected.

A component-level example: The control valve of the previous example represents the only path through which essential coolant can flow. The induced temperature fluctuations cause substantial error in the subsystem's product output, regardless of the power level selected. The only alternative is to shut down the process for repair of the control valve.

3. Integrity Crisis. This condition involves a system facing imminent equipment damage. The strategy here is to invoke immediate protection of equipment and associated subsystems. Delivery of product would be suspended pending restoration.

A component-level example: The coolant flow control valve of the above examples has frozen shut, preventing any coolant flow to the subsystem's equipment. No other means of cooling is available. Without cooling, expensive equipment would be damaged within seconds. Therefore immediate shutdown is required.

The homeostatic regions and transition corridors are normally enveloped by the degraded region. This region may be entered either by a change in system state (i.e., system state traversing the boundary separating the regions) or by redefinition of the homeostatic region (i.e., a receding of the boundary, thus leaving the system state in the degraded region). In the former case, a component failure itself may be incipient or as yet unobserved, although its effect on the process would be to drive the state vector out of the homeostatic region. In the latter case, the failure may be observed before the system state has had an opportunity to change.

UNCONTROLLABLE REGION

A goal of the control system upon entering the uncontrollable region is to alert the plant operators that a controllability problem exists. Prior to entering this region, the control system should have been attempting to shut down or subdue the process. Entry into this region indicates that the procedures or rules used while in the degraded region were ineffective. Further, the control system may have exhausted its ability or resources to control or restrain the situation. A subsystem whose state vector is in the uncontrollable region may exhibit one of several behaviors: (1) the subsystem is on a trajectory to an undesirable, possibly destructive state and is unresponsive to commands from the control system; (2) the system is static and in an undesirable state, also unresponsive to commands from the control system; or (3) the subsystem is chaotic, in which case very small control command changes produce large swings in the system's response, and the cause and effect relationship may appear illogical (i.e., true mathematically chaotic behavior). Several situations may have caused the state of the system to move to the uncontrollable region from the degraded region. The designer's understanding of the behavior of the system was incomplete or in error, or failures occurred beyond the scope of the system's design and outside its fault-tolerant capability.

Surrounding the uncontrollable region are the initiators of the plant safety and protection systems as shown in Fig. 1a. Failure of the control system to regain control of the process should eventually invoke a safety system response. However, the same failures or damage that impeded control action and led the system to the uncontrollable region might also prevent effective safety action, as would common-mode failure of shared equipment.

## PHASED APPROACH TO CONTROL SYSTEM DESIGN

The goals of automating a nuclear plant can be viewed as time-oriented layers:

1. Extend reactor core life as long as possible to decrease downtime and enhance fuel conversion;
2. Minimize wear on plant components to increase their service life;
3. Protect equipment, facilities, and instrumentation from damage;
4. Provide turbine-generator output power demanded;
5. Keep plant parameters within design specification and away from safety trips (i.e., adequate safety margin);
6. Minimize control actions required to accomplish control objectives; and
7. Maintain the stability of the process.

These goals become the operational objectives of the various control modules in the plant control system hierarchy. To meet these goals requires an intelligent control system that goes beyond traditional feedback-controlled regulation. One can view the merging of intelligence with a control system as moving operator knowledge and skill into the realm of system software. This should lead to improved diagnostic and decision-making capability as well as facilitate operator understanding of some internal processes of the control system.

Design of an automated system that can accomplish all of the objectives and functions discussed thus far represents a complex and time-consuming program. Like all large tasks, however, it can be partitioned into more manageable subtasks. This can be accomplished by progressive development of the system design. The progression can be thought of as a series of logical phases in the unfolding of the design; each phase adds another layer of intelligence to the control system. The phases follow somewhat the dimensions of automation. They are described as logical, not necessarily chronological, although in reality design would progress through the phases in a sequence with iteration.

In Phase 1, the basic control and automatic actions of the control system are developed. This phase of design does not have to account for failure of equipment. In a sense, the plant components are assumed perfect, requiring neither maintenance nor repair. Design thus concentrates on maintaining the stability of the processes and on automatic execution of actions to maneuver the plant through various states to the target state with its associated power level. Also, tolerance to noise and minor disturbances are considered. In this phase a structure emerges that will be amended and expanded in the subsequent phases.

In Phase 2, the basic control structure of Phase 1 is amended and expanded by including the tasks of subsystem and equipment testing and validation. Analysis of operating procedures reveals that a sizable portion of operator startup and shutdown tasks are related to verification of equipment availability, condition, and mode.

In Phase 3, the system emerging from Phase 2 is amended and expanded by including decision-making capability and required actions for coping with contingencies. Some contingency actions, closely associated with the basic control of certain pieces of equipment, may have been included in Phase 1 design. Phase 3, however, is mostly devoted to improving plant response in the degraded state so as to return the plant to a productive state and prevent it from lapsing into the uncontrollable region. The design emerging from Phase 3 employs features that can recognize a problem and select or devise a procedure or plan to restore the plant to normal operation.

In Phase 4, maintenance and calibration functions are added to the structure of the Phase 3 control system. Limited use of robotic devices may allow automation of many maintenance and calibration procedures; however, because of a particular need for human dexterity to reach and manipulate equipment, a Phase 4 system may not come into being until far in the future.

## CONCLUSION

The control techniques described have been applied elsewhere to the study of a nuclear system. Some of the underlying philosophy has been discussed here. Increased automation possessing intelligent control capability under various degrees of equipment degradation is needed and possible. Such improvements can be accomplished using a phased approach to control system design and structured software design techniques.

Certain aspects of the high-level, decision-making capabilities of automated control systems, especially for some complicated degraded operations, are at the limits of current software capabilities. Nevertheless, an improvement in control system function and design would result from the implementation of automated control with limited maneuverability in the event of equipment failure or degradation.

## REFERENCES


1. R. A. Kisner and P. R. Frey, Functions and Operations of Nuclear Power Plant Crews, Oak Ridge National Laboratory Report NUREG/CR-2587, ORNL/TM-8237, 1982.

2. R. Pulliam et al., A Methodology for Allocating Nuclear Power Plant Control Functions to Human or Automatic Control, Oak Ridge National Laboratory Report NUREG/CR-3331, ORNL/TM-8781, 1983.

3. E. Yourdon and L. L. Constantine, Structured Design: Fundamentals of a Discipline of Computer Program and Systems Design, Prentice-Hall, 1979.

4. J. Zaborsky, "Digital Control of the Large Electric Power System in Normal and Emergency State Operation by Decision and Control," Partial Collection of Publications from Research Conducted at Department of Systems Science and Mathematics, Washington University, St. Louis, Mo. (no date available).

5. R. W. Colley, Alternative Strategies for the Procedure Prompting System, Hanford Engineering Development Laboratory Report HEDL-PC-2398, 1983.


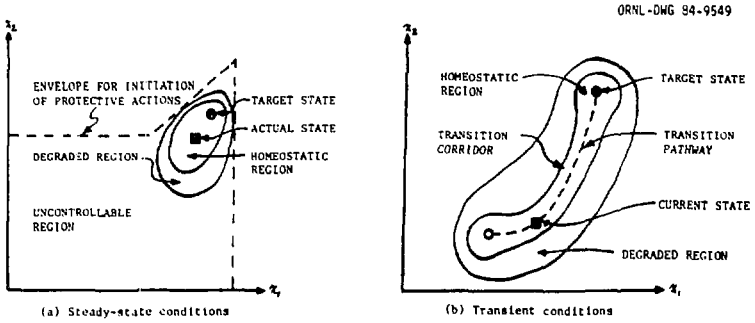


Fig. 1. Control regions in state space.